ASSURANCE ACTIVITY REPORT

High Sec Labs SK41PHU-4, DK42PHU-4, SX42PHU-4, SX82PHU-4, SC42DHU-4, SC42PHU-4 Firmware Version 44444-E7E7 Peripheral Sharing Devices

PREPARED BY

EWA-Canada, An Intertek Company

PREPARED FOR

Communications Security Establishment (CSE) and
National Information Assurance Partnership (NIAP)

REPORT NO

2149-002-D007-1

DOCUMENT VERSION

Version 1.0

DATE

20 December 2022

Contents

1 INTRODUCTION 1

1.1 EVIDENCE 1

1.2 REFERENCES 2

2 SECURITY FUNCTIONAL REQUIREMENT ASSURANCE ACTIVITIES 3

2.1 USER DATA PROTECTION (FDP) 3

2.1.1 FDP_APC_EXT.1 Active PSD Connections 3

2.1.2 FDP_APC_EXT.1/AO Active PSD Connections 4

2.1.3 FDP_APC_EXT.1/KM Active PSD Connections 11

2.1.4 FDP_APC_EXT.1/UA Active PSD Connections 20

2.1.5 FDP_APC_EXT.1/VI Active PSD Connections 25

2.1.6 FDP_FIL_EXT.1/UA Device Filtering (User Authentication Devices) 34

2.1.7 FDP_PDC_EXT.1 Peripheral Device Connection 37

2.1.8 FDP_PDC_EXT.2/AO Peripheral Device Connection (Audio Output) 46

2.1.9 FDP_PDC_EXT.2/KM Authorized Devices (Keyboard/Mouse) 48

2.1.10 FDP_PDC_EXT.3/KM Authorized Connection Protocols (Keyboard/Mouse) 49

2.1.11 FDP_PDC_EXT.2/UA Authorized Devices (User Authentication Devices) 50

2.1.12 FDP_PDC_EXT.4 Supported Authentication Device 51

2.1.13 FDP_PDC_EXT.2/VI Peripheral Device Connection (Video Output) 51

2.1.14 FDP_PDC_EXT.3/VI Authorized Connection Protocols (Video Output) 53

2.1.15 FDP_PUD_EXT.1 Powering Unauthorized Devices 54

2.1.16 FDP_PWR_EXT.1 Powered By Computer 55

2.1.17 FDP_SWI_EXT.1 PSD Switching 56

2.1.18 FDP_RIP_EXT.1 Residual Information Protection 57

2.1.19 FDP_TER_EXT.1 Session Termination 58

2.1.20 FDP_UAI_EXT.1 User Authentication Isolation 58

2.1.21 FDP_UDF_EXT.1/AO Unidirectional Data Flow (Audio Output) 61

2.1.22 FDP_UDF_EXT.1/KM Unidirectional Data Flow (Keyboard/Mouse) 63

2.1.23 FDP_UDF_EXT.1/VI Unidirectional Data Flow (Video Output) 64

2.1.24 FDP_AFL_EXT.1 Audio Filtration 64

2.2 PROTECTION OF THE TSF (FPT) 66

2.2.1 FPT_FLS_EXT.1 Failure with Preservation of Secure State 66

2.2.2 FPT_NTA_EXT.1 No Access to TOE ... 66
2.2.3 FPT_PHP.1 Passive Detection of Physical Attack ... 67
2.2.4 FPT_TST.1 TSF Testing ... 68
2.2.5 FPT_TST_EXT.1 TSF Testing ... 70
3 EVALUATION ACTIVITIES FOR OPTIONAL REQUIREMENTS ... 72
3.1 USER DATA PROTECTION (FDP) ... 72
3.1.1 FDP_FIL_EXT.1/KM Device Filtering (Keyboard/Mouse) ... 72
3.1.2 FDP_RDR_EXT.1 Re-Enumeration Device Rejection ... 74
3.1.3 FDP_RIP_EXT.2 Purge of Residual Information ... 75
3.2 PROTECTION OF THE TSF (FPT) ... 77
3.2.1 FPT_PHP.3 Resistance to Physical Attack ... 77
4 SELECTION-BASED REQUIREMENTS ... 78
4.1 SECURITY AUDIT (FAU) ... 78
4.1.1 FAU_GEN.1 Audit Data Generation ... 78
4.2 USER DATA PROTECTION (FDP) ... 81
4.2.1 FDP_CDS_EXT.1 Connected Displays Supported ... 81
4.2.2 FDP_IPC_EXT.1 Internal Protocol Conversion ... 82
4.2.3 FDP_SWI_EXT.3 Tied Switching ... 82
4.2.4 FDP_RIP.1/KM Residual Information Protection (Keyboard Data) ... 83
4.2.5 FDP_SPR_EXT.1/DP Sub-Protocol Rules (DisplayPort Protocol) ... 84
4.2.6 FDP_SPR_EXT.1/DVI-D Sub-Protocol Rules (DVI-D Protocol) ... 85
4.2.7 FDP_SPR_EXT.1/HDMI Sub-Protocol Rules (HDMI Protocol) ... 86
4.2.8 FDP_SWI_EXT.2 PSD Switching Methods ... 87
4.2.9 FDP_TER_EXT.2 Session Termination of Removed Devices ... 88
4.2.10 FDP_TER_EXT.3 Session Termination upon Switching ... 89
4.3 IDENTIFICATION AND AUTHENTICATION (FIA) ... 90
4.3.1 FIA_UAU.2 User Authentication Before Any Action ... 90
4.3.2 FIA_UID.2 User Identification Before Any Action ... 91
4.4 SECURITY MANAGEMENT (FMT) ... 91
4.4.1 FMT_MOF.1 Management of Security Functions Behavior ... 91
4.4.2 FMT_SMF.1 Specification of Management Functions ... 93
4.4.3 FMT_SMR.1 Security Roles ... 95
4.5 PROTECTION OF THE TSF (FPT) ... 95
4.5.1 FPT_STM.1 Reliable Time Stamps ... 95

4.6 TOE ACCESS (FTA) 96

4.6.1 FTA_CIN_EXT.1 Continuous Indications 96

5 SECURITY ASSURANCE REQUIREMENT ACTIVITIES 99

5.1 DEVELOPMENT (ADV) 99

5.1.1 ADV_FSP.1 Basic Functional Specifications 99

5.2 GUIDANCE DOCUMENTS (AGD) 99

5.2.1 AGD_OPE.1 Operational User Guidance 99

5.2.2 AGD_PRE.1 Preparative Procedures 99

5.3 LIFE-CYCLE SUPPORT (ALC) 100

5.3.1 ALC_CMC.1 Labeling of the TOE 100

5.3.2 ALC_CMS.1 TOE CM Coverage 100

5.4 TESTS (ATE) 100

5.4.1 ATE_IND Independent Testing - Conformance 100

5.5 VULNERABILITY ANALYSIS (AVA) 101

5.5.1 AVA_VAN.1 Vulnerability Survey 101

The Developer of the TOE:

High Sec Labs Ltd.
29 Haeshel St
Caesarea,
Israel 3079510

Common Criteria Versions

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017.

Common Evaluation Methodology Versions

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017.

Protection Profiles

- Protection Profile for Peripheral Sharing Device, 2019-07-19, Version 4.0
- PP-Module for Analog Audio Output Devices, 2019-07-19, Version 1.0
- PP-Module for Keyboard/Mouse Devices, 2019-07-19, Version 1.0
- PP-Module for User Authentication Devices, 2019-07-19, Version 1.0
- PP-Module for Video/Display Devices, 2019-07-19, Version 1.0
- PP-Configuration for Peripheral Sharing Device, Analog Audio Output Devices, Keyboard/Mouse Devices, User Authentication Devices, and Video/Display Devices, 19 July 2019, Version 1.0

NIAP Technical Decisions

ITEM	TECHNICAL DECISION TITLE
TD0506	Missing steps to connect and reconnect display [MOD_VI_V1.0]
TD0507	Clarification on USB plug type [MOD_KM_V1.0]
TD0514	Correction to MOD_VI FDP_APC_EXT.1 Test 3 Step 6 [MOD_VI_V1.0]
TD0518	Typographical error in Dependency Table [PP_PSD_V4.0]

ITEM	TECHNICAL DECISION TITLE
TD0539	Incorrect selection trigger in FTA_CIN_EXT.1 in [MOD_VI_V1.0]
TD0557	Correction to Audio Filtration Specification table in FDP_AFL_EXT.1 [MOD _AO_v1.0]
TD0583	FPT_PHP.3 modified for PSD remote controllers [PP_PSD_V4.0]
TD0584	Update to FDP_APC_EXT.1 Video Tests [MOD_VI_V1.0]
TD0585	Update to FDP_APC_EXT.1 Audio Output Tests [MOD_AO_V1.0]
TD0586	DisplayPort and HDMI Interfaces in FDP_IPC_EXT.1 [MOD_VI_V1.0]
TD0593	Equivalency arguments for PSD [MOD_AO_V1.0], [MOD_KM_V1.0], [MOD_VI_V1.0]
TD0619	Test EAs for internal UA devices [MOD_UA_V1.0]
TD0620	EDID Read Requirements [MOD_VI_V1.0]

Table 1 – NIAP Technical Decisions

1 Introduction

This document presents assurance activity evaluation results of the TOE evaluation. There are three types of assurance activities and the following is provided for each:

1. TOE Summary Specification (TSS) - An indication that the required information is in the TSS section of the Security Target;
2. Guidance - A specific reference to the location in the guidance is provided for the required information; and
3. Test – A summary of the test procedure used and the results obtained is provided for each required test activity.

This Assurance Activities Report contains sections for each functional class and family and sub-sections addressing each of the SFRs specified in the Security Target. The SARs are also addressed.

1.1 Evidence

The following is a list of the documents consulted:

- [ST] High Sec Labs SK41PHU-4, DK42PHU-4, SX42PHU-4, SX82PHU-4, SC42DHU-4, SC42PHU-4 Firmware Version 44444-E7E7 Peripheral Sharing Devices Security Target, Version 1.0, 20 December 2022

- [CC_Supp] High Sec Labs SK41PHU-4, DK42PHU-4, SX42PHU-4, SX82PHU-4, SC42DHU-4, SC42PHU-4 Firmware Version 44444-E7E7 Peripheral Sharing Devices Common Criteria Guidance Supplement, version 1.4, 20 December 2022

- [Isol] High Sec Labs SK41PHU-4, DK42PHU-4, SX42PHU-4, SX82PHU-4, SC42DHU-4, SC42PHU-4 Firmware Version 44444-E7E7 Peripheral Sharing Devices Isolation Document, version 1.3, 18 June 2021

- [19959] HSL Quick Installation Guide 2/4/8 Ports High Security DP/HDMI KVM Switches, HDC19959 Rev 1.0

- [19961] HSL Quick Installation Guide 4/8 Ports High Security DP/HDMI Mini-Matrix KVM Switches, HDC19961 Rev 1.0

- [20601] HSL Quick Installation Guide 4 Ports High Security KVM Combiner Switches, HDC20601 Rev 1.0

- [19969] High Sec Labs 4/8 Port Auxiliary Front Panel, HDC19969 Rev 1.0

- [ADMIN] HSL Administrator Guide, HDC19968, Rev. C

- [ETProcRes] EVALUATION TEST PLAN, PROCEDURES AND TEST RESULTS FOR PERIPHERAL SHARING DEVICE VERSION 4.0 COMMON CRITERIA EVALUATION OF HSL CFG_PSD-AO-KM-UA-VI, version 1.2, 20 December 2022

1.2 References

- [PP_PSD_V4.0] Protection Profile for Peripheral Sharing Device, 2019-07-19, Version 4.0
- [MOD_AO_V1.0] PP-Module for Analog Audio Output Devices, 2019-07-19, Version 1.0
- [MOD_AO_SD] Supporting Document, PP-Module for Analog Audio Output Devices, 2019-07-19, Version 1.0
- [MOD_KM_V1.0] PP-Module for Keyboard/Mouse Devices, 2019-07-19, Version 1.0
- [MOD_KM_SD] Supporting Document, PP-Module for Keyboard/Mouse Devices, 2019-07-19, Version 1.0
- [MOD_UA_V1.0] PP-Module for User Authentication Devices, 2019-07-19, Version 1.0
- [MOD_UA_SD] Supporting Document, PP-Module for User Authentication Devices, 2019-07-19, Version 1.0
- [MOD_VI_V1.0] PP-Module for Video/Display Devices, 2019-07-19, Version 1.0
- [MOD_VI_SD] Supporting Document, PP-Module for Video/Display Devices, 2019-07-19, Version 1.0

2 Security Functional Requirement Assurance Activities

2.1 User Data Protection (FDP)

2.1.1 FDP_APC_EXT.1 Active PSD Connections

2.1.1.1 FDP_APC_EXT.1.1

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

Evaluation activities are detailed below.

2.1.1.2 FDP_APC_EXT.1.2

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

Evaluation activities are detailed below.

2.1.1.3 FDP_APC_EXT.1.3

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

Evaluation activities are detailed below.

2.1.1.4 FDP_APC_EXT.1.4

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

Evaluation Activity

Isolation Document

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.

TSS

The evaluator shall verify that the TSS describes the conditions under which the TOE enters a failure state.

Guidance

The evaluator shall verify that the operational user guidance describes how a user knows when the TOE enters a failure state.

Test

There are no test Evaluation Activities for this component.

Isolation Document Evaluator Assessment:

The High Sec Labs SK41PHU-4, DK42PHU-4, SX42PHU-4, SX82PHU-4, SC42DHU-4, SC42PHU-4 Firmware Version 44444-E7E7 Peripheral Sharing Devices Isolation Document, June 18, 2021, v1.3 was reviewed. This document adequately describes the proper isolation whether the TOE is powered on or not. A complete review of this document is in the file “CFG_PSD-AO-KM-UA-VI - Annex D HSL Isolation Documentation assessment”.

TSS Evaluator Assessment:

Section 9.4 of the TSS discusses the conditions under which the TOE enters a failure state due to self-test failure.

Guidance Evaluator Assessment:

The [ADMIN], [19959], [19961], [19968] and [20601] explains the possible errors and failures and the behavior of the device when in a fail state. Each of the Quick Installation Guides also states what causes a device to enter a fail state.

Test Evaluator Assessment:

NA

2.1.2 FDP_APC_EXT.1/AO Active PSD Connections

2.1.2.1 FDP_APC_EXT.1.1/AO

The TSF shall route user data only from the interfaces selected by the user.

Evaluation activities are detailed below.

2.1.2.2 FDP_APC_EXT.1.2/AO

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

Evaluation activities are detailed below.

2.1.2.3 FDP_APC_EXT.1.3/AO

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

Evaluation activities are detailed below.

2.1.2.4 FDP_APC_EXT.1.4/AO

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

Application Note

This SFR is refined from the PSD PP for this PP-Module to include further restrictions on how data may be routed in regards to interfaces selected by the user.

This SFR is refined from the PSD PP for this PP-Module to include further restrictions for electrical signals. Electrical signals are considered not to flow between connected computers and data is considered not to transit the TOE if no signal greater than 45dB of attenuation at the extended audio frequency range is received. It is very unlikely that this element can be satisfied unless all unselected computer interfaces are shorted to ground by the TSF.

Note that the above port-to-port attenuation pass criterion is calculated based on the following: 45 dBv = 177.82 signal to voltage ratio. When the signal inserted on one TOE computer interface audio input is 2.00 V peak-to-peak sine wave, the maximum allowed output signal voltage measured at another TOE computer interface is therefore 11.2mV (or well below noise level). Negative swing is measured when the generated audio signal average voltage is 0V.

If the peripheral interface supports multiple signals (such as right and left audio, or audio bias), then all those supported signals should comply with the above SFRs.

If the TOE claims conformance to multiple PP-Modules, each PP-Module modifies this SFR in a different manner for the interfaces that are unique to that module. In this case, the ST author should reference this modification of the SFR as "FDP_APC_EXT.1/AO" for uniqueness. Note that all elements of FDP_APC_EXT.1 must be included in this iteration, not just the ones that are modified by this PP Module.

Evaluation Activity

Isolation Document

The evaluator shall examine the Isolation Documentation to determine that it describes the logic under which the TSF permits audio flows from a connected computer to a connected audio output interface.

The evaluator shall examine the Isolation Documentation to determine that it describes how the TOE enforces audio output data flow isolation from other TOE functions, such that it is not possible for two computers connected to the TOE to use the TOE to communicate with one another. The description shall ensure the signal attenuation in the extended audio frequency range between any computer audio output interfaces is at least 45 dB measured with a 2V input pure sine wave at the extended audio frequency range, including negative swing signal.

The evaluator shall examine the Isolation Documentation to determine that it describes how the TOE prevents the audio output signal from traversing the TOE while the TOE is powered off.

TSS

There are no additional TSS activities for this component.

Guidance

If the ability of the TOE to grant or deny authorization to audio communications is configurable, the evaluator shall verify that the operational guidance describes how to configure the TSF to behave in the manner specified by the SFR. This includes the possibility of both administratively configured TOE settings and any peripherals/connectors that are included with the TOE that cause data flows to behave differently if peripherals are connected through them.

Test

Test Setup

The evaluator shall perform the following setup steps:

- Configure the TOE and the operational environment in accordance with the operational guidance.

- Play a different audio file on a number of computers for each TOE computer analog audio interface.

- Connect each computer to a TOE computer analog audio interface.

-Turn on the TOE.

Note that for a TOE that provides audio mixing function the evaluator shall maximize the volume on a specific channel where instructed in the following text to assign that specific computer.

Note: Electrical signals are considered not to flow between connected computers and data is considered not to transit the TOE if no signal greater than 45 dB of attenuation at the specific audio frequency is received

Test 1-AO – Analog Audio Output Data Routing Methods.

This test verifies the functionality of the TOE routing methods while powered on, powered off, and in failure state.

Step 1: Connect amplified speakers to the TOE audio output device interface. Set the speakers to approximately 25% volume.

Step 2: [Conditional: if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP, then] perform step 3 for each switching method selected in FDP_SWI_EXT.2.2 in accordance with the operational user guidance.

Step 3: For each connected computer, ensure it is selected, listen to the amplified speakers, and verify that the audio is coming from the selected computer(s). Adjust the volume if necessary.

Step 4: Replace the speakers with a computer connected to the TOE analog audio output device interface and run audio spectrum analyzer software on it. Run tone generator software on all connected computers.

Step 5: Turn off the TOE, and for each connected computer, use the tone generator program to generate a sine wave audio tone for each of the designated frequencies and verify that no audio is present in the audio spectrum analyzer software on the computer connected to the TOE analog audio output device interface.

Step 6: Power on the TOE, cause the TOE to enter a failure state, and verify that the TOE provides the user with an indication of *failure. For each connected computer use the tone generator program to generate a sine wave audio tone for each of the designated frequencies and verify that no audio is present in the audio spectrum analyzer software on the computer connected to the TOE analog audio output device interface.*

Test 2-AO – Analog Audio Output Interface Isolation

[Conditional: perform this test if "switching through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP.]

This test verifies that no data or electrical signals flow between connected computers while the TOE is powered on or off.

Step 1. Continue with the setup from Test 1.

Step 2: Connect a computer to the TOE analog audio output device interface. Run audio spectrum analyzer software on all computers.

Step 3: Perform steps 4-13 for each TOE analog audio computer interface.

Step 4: Turn on the TOE and ensure the first computer is selected.

Step 5: Use the tone generator program on the first computer to generate a sine wave audio tone for each of the designated frequencies. Verify that the audio is present in the audio spectrum analyzer software on the computer connected to the TOE analog audio output device interface and is not present in the audio spectrum analyzer software on any of the non-selected computers. This step does not fail if frequencies above 20 kHz are not present in the software on the connected computer due to attenuation as per FDP_AFL_EXT.1. ***Note: TD0585 applied***

Step 6: For each other TOE analog audio computer interface, select that computer and use the tone generator program on the first computer (now no longer selected) to generate a sine wave audio tone for each of the designated frequencies. Verify that the audio is not present in the audio spectrum analyzer software on the selected computer, the other non-selected computers, or the computer connected to the TOE analog audio output device interface.

Step 7: Power off the TOE and use the tone generator program on the first computer to generate a sine wave audio tone for each of the designated frequencies. Verify that the audio is not present in the audio spectrum analyzer software on any of the other connected computers.

Step 8: Restart the TOE, select the first computer, and replace it with an external audio signal generator.

Step 9: For each non-selected computer connected to the TOE analog audio output computer interface, replace it with an oscilloscope set to measure the peak-to-peak voltage and perform steps 10-14.

Step 10: Perform steps 11-13 with the signal generator set to the following settings:

- Pure sine wave around the average voltage of half output (positive signal only), with the output signal set to 2.00 V peak-to-peak, calibrating the signal with the oscilloscope as needed

- Signal average to 0v (negative swing)

Step 11: Set the signal generator to generate the designated frequencies and verify the signal on the oscilloscopes is 11.2 mV or less. This level of signal ensures signal attenuation of 45 dB in the extended audio frequency range.

Step 12: For each other TOE analog audio computer interface, select it, set the signal generator to generate the designated frequencies, and verify the signal on the oscilloscopes is 11.2 mV or less.

Step 13: Power off the TOE and set the signal generator to generate the designated frequencies and verify the signal on the oscilloscopes is 11.2 mV or less.

Test 3-AO – No Flow between Computers with Other Peripheral Device Types

[Conditional: Perform this test only if a PP-Module aside from the Analog Audio Output PP-Module is part of the PP-Configuration being claimed AND if "switching through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP.]

This test verifies that power events at one TOE USB computer interface do not affect the analog audio output computer interface of another computer.

Note: "No sound appears" is defined as a temporary jump of at least 4 dB from the existing ambient noise floor.

Step 1: Connect a computer to the TOE analog audio output peripheral interface and run audio spectrum analyzer software on it and each connected computer.

Step 2: Perform steps 3-9 for each connected computer.

Step 3: Ensure the first computer is selected and perform steps 4-8 while the TOE is powered on and powered off.

[Conditional: Perform steps 4 and 5 only if the PP-Module for Video/Display Devices is part of the PP Configuration being claimed.]

Step 4: For each other connected computer, disconnect and reconnect the video cables from the TOE computer interface several times. Verify that no sound appears on the audio analyzer software on the first computer.

Step 5: Disconnect and reconnect the first computer's video cables from the TOE computer interface several times. Verify that no sound appears on the audio analyzer software on the other connected computers.

Step 6: [Conditional: If the PP-Module for Keyboard/Mouse Devices or PP-Module for User Authentication Devices is part of the PP-Configuration being claimed, then:] for each other connected computer, disconnect and reconnect the USB cable from the TOE USB computer interface several times. Verify that no sound appears on the audio analyzer software on the computer connected to the TOE analog audio output peripheral interface or any connected computers.

Step 7: [Conditional: If the PSD PP-Module for Keyboard/Mouse Devices is part of the PP-Configuration being claimed, then:] disconnect and reconnect the peripheral device type(s) selected in FDP_PDC_EXT.3.1/KM from the TOE KM peripheral device interface several times. Verify that no sound appears on the audio analyzer software on the other connected computers.

Step 8: [Conditional: If the PP-Module for User Authentication Devices is part of the PP-Configuration being claimed and "external" is selected in FDP_PDC_EXT.4.1, then:] disconnect and reconnect the UA peripheral device from the TOE UA peripheral device interface several times. Verify that no sound appears on the audio analyzer software on the other connected computers.

Step 9: [Conditional: If the PP-Module for User Authentication Devices is part of the PP-Configuration being claimed, then:] connect an authentication session to the first computer and verify that no sounds appears on the audio analyzer software on the other connected computers.

Test 4-AO – No Flow between Connected Computers over Time

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 Analog Audio Output port.

Step 1: Ensure only one computer is connected and it is selected. Run a tone generator program on the connected computer and the audio analyzer software on a non-connected computer.

Step 2: Perform steps 3-11 while the TOE is powered on and powered off.

Step 3: Perform steps 4-5 for each of the designated frequencies.

Step 4: Use the tone generator program on the connected computer to generate a sine wave audio tone.

Step 5: Disconnect the connected computer, wait two minutes, connect the other computer, and verify that the generated audio frequency is not present in the audio spectrum analyzer software.

Step 6: Replace the connected computer with an external audio signal generator.

Step 7: Perform steps 8-11 with the signal generator set to the following settings:

- Pure sine wave around the average voltage of half output (positive signal only), with the output signal set to 2.00 V peak-to-peak, calibrating the signal with the oscilloscope as needed

- Signal average to 0v (negative swing)

Step 8: Perform steps 9-11 for each of the designated frequencies.

Step 9: Use the signal generator to generate the signal.

Step 10: Disconnect the signal generator, wait two minutes, and replace it with an oscilloscope set to measure the peak-to-peak voltage

Step 11: Verify the signal on the oscilloscope is 11.2 mV or less at the generated frequency.

Isolation Document Evaluator Assessment:

[Isol] has 2 figures, (figure 1 and figure2) that illustrate all possible data flows. There follows a table, Table 1 Data Flow Description, that gives an explanation of all data flows. Figures 3, 4 ,5, 6, 7 and 9 which characterize the data flows for various parts of the TOE (i.e. combiners, switches, etc.) are part of the isolation justification and indicate the methods used to maintain the data separation. Section 2.3 of [Isol] gives an explanation of all data flow isolation. Section 2.4 discusses power isolation. Section 3 describes the isolation enforcement policy for various aspects of the TOE. Figure 8 shows the physical characteristics. The file CFG_PSD-AO-KM-UA-VI - Annex D HSL Isolation Documentation assessment.doc is an analysis of the Isolation document.

TSS Evaluator Assessment:

NA

Guidance Evaluator Assessment:

The evaluator examined the product Quick Installation Guides [19959], [19961], [19968] and [20601] to determine the verdict of this evaluation activity. Each guidance document gives instructions on how to install the TOE properly. The ability to grant or deny authorization to audio communications is not configurable.

Test Evaluator Assessment:

Test 1

1. Connect amplified speakers to the TOE audio output device interface. Set the speakers to approximately 25% volume.
2. *[Conditional: if “switching can be initiated only through express user action” is selected in FDP_SWI_EXT.1.1 in the PSD PP, then]* perform step 3 for each switching method selected in FDP_SWI_EXT.2.2 in accordance with the operational user guidance.
3. Play an audio file on the computer, then listen to the amplified speakers, and verify that the audio is coming from the selected computer(s). Adjust the volume if necessary.
4. Replace the speakers with a computer connected to the TOE analog audio output device interface and run audio spectrum analyzer software on it. Run tone generator software on all connected computers.
5. Turn off the TOE, and for each connected computer, use the tone generator program to generate a sine wave audio tone for each of the designated frequencies and verify that no audio is present in the audio spectrum analyzer software on the computer connected to the TOE analog audio output device interface.
6. Power on the TOE, cause the TOE to enter a failure state, as per the TOE guidance. For each connected computer use the tone generator program to generate a sine wave audio tone for each of the designated frequencies (14Khz-20Khz, 30Khz, 40Khz, 50Khz, 60Khz) and verify that no audio is present in the audio spectrum analyzer software on the computer connected to the TOE analog audio output device interface.

The functionality of the TOE’s routing methods has been tested while powered on, powered off, and in failure state. The evaluator confirmed that audio is only routed to selected authorized computers.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 2

1. Continue with the setup from Test 1.
2. Connect a computer to the TOE analog audio output device interface. Run audio spectrum analyzer software on all computers.
3. Perform steps 4-13 for each TOE analog audio computer interface.
4. Turn on the TOE and ensure the first computer is selected.
5. Use the tone generator program on the first computer to generate a sine wave audio tone for each of the designated frequencies. Verify that the audio is present in the audio spectrum analyzer software on the computer connected to the TOE analog audio output device interface and is not present in the audio spectrum analyzer software on any of the non-selected computers. This step does not fail if frequencies above 20 kHz are not present in the software on the connected computer due to attenuation as per FDP_AFL_EXT.1. Note: TD0585 applied
6. For each other TOE analog audio computer interface, select that computer and use the tone generator program on the first computer (now no longer selected) to generate a sine wave audio tone for each of the designated frequencies. Verify that the audio is not present in the audio spectrum analyzer software on the selected computer, the other non-selected computers, or the computer connected to the TOE analog audio output device interface.
7. Power off the TOE and use the tone generator program on the first computer to generate a sine wave audio tone for each of the designated frequencies. Verify that the audio is not present in the audio spectrum analyzer software on any of the other connected computers.
8. Restart the TOE, select the first computer, and replace it with an external audio signal generator.
9. For each non-selected computer connected to the TOE analog audio output computer interface, replace it with an oscilloscope set to measure the peak-to-peak voltage and perform steps 10-14.
10. Perform steps 11-13 with the signal generator set to the following settings: Pure sine wave around the average voltage of half output (positive signal only), with the output signal set to 2.00 V peak-to-peak, calibrating the signal with the oscilloscope as needed Signal average to 0v (negative swing).
11. Set the signal generator to generate the designated frequencies and verify the signal on the oscilloscopes is 11.2 mV or less. This level of signal ensures signal attenuation of 45 dB in the extended audio frequency range.
12. For each other TOE analog audio computer interface, select it, set the signal generator to generate the designated frequencies, and verify the signal on the oscilloscopes is 11.2 mV or less.
13. Power off the TOE and set the signal generator to generate the designated frequencies and verify the signal on the oscilloscopes is 11.2 mV or less.

No data or electrical signals flow between connected computers while the TOE is powered on or off. The evaluator has confirmed that audio is only present on the selected computer and does not leak to other connected computers.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 3

1. Connect a computer to the TOE analog audio output peripheral interface and run audio spectrum analyzer software on it and each connected computer.
2. Perform steps 3-9 for each connected computer.

3. Ensure the first computer is selected and perform steps 4-8 while the TOE is powered on and powered off.
4. For each other connected computer, disconnect and reconnect the video cables from the TOE computer interface several times. Verify that no sound appears on the audio analyzer software on the first computer.
5. Disconnect and reconnect the first computer's video cables from the TOE computer interface several times. Verify that no sound appears on the audio analyzer software on the other connected computers.
6. *[Conditional: If the PP-Module for Keyboard/Mouse Devices or PP-Module for User Authentication Devices is part of the PP-Configuration being claimed, then:]* for each other connected computer, disconnect and reconnect the USB cable from the TOE USB computer interface several times. Verify that no sound appears on the audio analyzer software on the computer connected to the TOE analog audio output peripheral interface or any connected computers.
7. *[Conditional: If the PSD PP-Module for Keyboard/Mouse Devices is part of the PP-Configuration being claimed, then:]* disconnect and reconnect the peripheral device type(s) selected in FDP_PDC_EXT.3.1/KM from the TOE KM peripheral device interface several times. Verify that no sound appears on the audio analyzer software on the other connected computers.
8. *[Conditional]: If the PP-Module for User Authentication Devices is part of the PP-Configuration being claimed and "external" is selected in FDP_PDC_EXT.4.1, then:]* disconnect and reconnect the UA peripheral device from the TOE UA peripheral device interface several times. Verify that no sound appears on the audio analyzer software on the other connected computers.
9. *[Conditional: If the PP-Module for User Authentication Devices is part of the PP-Configuration being claimed, then:]* connect an authentication session to the first computer and verify that no sounds appears on the audio analyzer software on the other connected computers.

The evaluator has confirmed that power events at one TOE USB computer interface do not affect the analog audio output computer interface of another computer.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 4

1. Ensure only one computer is connected and it is selected. Run a tone generator program on the connected computer and the audio analyzer software on a non-connected computer.
2. Perform steps 3-11 while the TOE is powered on and powered off.
3. Perform steps 4 - 5 for each of the designated frequencies.
4. Use the tone generator program on the connected computer to generate a sine wave audio tone.
5. Disconnect the connected computer, wait two minutes, connect the other computer, and verify that the generated audio frequency is not present in the audio spectrum analyzer software.
6. Replace the connected computer with an external audio signal generator.
7. Perform steps 8-11 with the signal generator set to the following settings: 11 Pure sine wave around the average voltage of half output (positive signal only), with the output signal set to 2.00 V peak-to-peak, calibrating the signal with the oscilloscope as needed Signal average to 0v (negative swing).
8. Perform steps 9 - 11 for each of the designated frequencies.
9. Use the signal generator to generate the signal.

10. Disconnect the signal generator, wait two minutes, and replace it with an oscilloscope set to measure the peak-to-peak voltage.
11. Verify the signal on the oscilloscope is 11.2 mV or less at the generated frequency.

The evaluator verified that the TOE does not send data to different computers connected to the same interface at different times.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

2.1.3 FDP_APC_EXT.1/KM Active PSD Connections

2.1.3.1 FDP_APC_EXT.1.1/KM

The TSF shall route user data only to the interfaces selected by the user.

Evaluation activities are detailed below.

2.1.3.2 FDP_APC_EXT.1.2/KM

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

Evaluation activities are detailed below.

2.1.3.3 FDP_APC_EXT.1.3/KM

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

Evaluation activities are detailed below.

2.1.3.4 FDP_APC_EXT.1.4/KM

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

Application Note

This SFR is refined from the PSD PP for this PP-Module to include further restrictions for electrical signals. It is unlikely that this element can be satisfied unless mouse and keyboard peripheral device interfaces are electrically and logically isolated from the connected computer interfaces or through other methods, such as USB host and USB device emulation.

For TOEs that support only a keyboard or mouse, but not both, tests and portions of tests that involve using the non-supported peripheral are considered conditional.

If the TOE claims conformance to multiple PP-Modules, each PP-Module modifies this SFR in a different manner for the interfaces that are unique to that module. In this case, the ST author should reference this modification of the SFR as "FDP_APC_EXT.1/KM" for uniqueness. Note that all elements of FDP_APC_EXT.1 must be included in this iteration, not just the ones that are modified by this PP-Module.

Evaluation Activity

Isolation Document

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).*

TSS

There are no TSS EAs for this component beyond what the PSD PP requires.

Guidance

There are no guidance EAs for this component beyond what the PSD PP requires.

Test

For tests that use the USB sniffer or USB analyzer software, the evaluator verifies whether traffic is sent or not sent by inspection of the passing USB transactions and ensuring they do not contain USB data payloads other than any expected traffic, as well as USB NAK transactions or system messages. To avoid clutter during USB traffic capture, the evaluator may filter NAK transactions and system messages.

The evaluator shall perform the following tests:

Test 1-KM – KM Switching methods

[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.

Step 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.

Step 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.

Step 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.

Step 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.

Step 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 - #*

Step 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.

Step 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.

Test 2-KM – Positive and Negative Keyboard and Mouse Data Flow Rules Testing

This test verifies the functionality for correct data flows of a mouse and keyboard during different power states of the selected computer.

Step 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.

Step 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.]

Step 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.

Step 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.

Step 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.

Step 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.

Step 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.

Step 8: Reboot the selected computer. Examine the USB protocol analyzers on each one of the nonselected computers and verify that no traffic is sent.

Step 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.

Step 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.

Step 11: Perform step 12 when the TOE is off and then in a failure state.

Step 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.

Test 3-KM – Flow Isolation and Unidirectional Rule

This test verifies that the TOE properly enforces unidirectional flow and isolation.

Step 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.

Step 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]

Step 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.

Step 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]

Step 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.

Step 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.

Step 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.

Step 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).

Step 9: Turn the TOE off and disconnect the peripheral devices connected in step 6.

Step 10: Reconnect the first computer interface USB cable to the TOE.

Step 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.

Step 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.

Test 4-KM – No Flow between Computer Interfaces

[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.

Step 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.

Step 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.

Step 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.

Step 4: Ensure the TOE is switched to the first computer.

Step 5: Reboot the first computer. Verify that no USB traffic is captured on all non-selected computer USB protocol analyzers.

Step 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.

Step 7: Perform steps 8 and 9 for each TOE keyboard/mouse peripheral interface.

Step 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.

Step 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. ***Note: TD0507 applied***

Step 10: Turn off the TOE. Verify that no new traffic is captured.

Test 5-KM – No Flow between Connected Computers over Time

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.

Step 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.

Step 2: Connect the first computer to the TOE and ensure it is selected and that no other computers are connected.

Step 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.

Step 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.

Step 5: Cease generation of the USB HID traffic, connect the second computer to the same port and ensure it is selected.

Step 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.

Step 7: Reboot the TOE and repeat step 6.

Step 8: Turn off the TOE and repeat step 6.

Step 9: Restart the TOE and repeat step 6.

Step 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.

Isolation Document Evaluator Assessment:

[Isol] has 2 figures, (figure 1 and figure2) that illustrate all possible data flows. There follows a table, Table 1 Data Flow Description, that gives an explanation of all data flows. Figures 3, 4 ,5, 6, 7 and 9 which characterize the data flows various parts of the TOE (i.e. combiners, switches, etc.) are part of the isolation justification and indicate the methods used to maintain the data separation. Section 2.3 Figure 3 of [Isol] gives an explanation of all data flow isolation. Section 2.4 discusses power isolation. Section 3 describes the isolation enforcement policy for various aspects of the TOE. Figure 8 shows the physical characteristics. A complete analysis of the Isolation document is found in the file CFG_PSD-AO-KM-UA-VI - Annex D HSL Isolation Documentation assessment.doc.

TSS Evaluator Assessment:

NA

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

Test 1

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.

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.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 2

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.

3. *[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.]* [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.

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.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 3

1. Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance.
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.
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.
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.

    This test step was not performed, since the keyboard and mouse correctly appeared in the listed devices in the device manager.

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.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 4

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. Note: TD0507 applied
10. Turn off the TOE. Verify that no new traffic is captured.

Correct data flow while the TOE is powered on or powered off has been tested. The evaluator confirmed that USB traffic is only captured on selected authorized computers.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 5

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.

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.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

2.1.4 FDP_APC_EXT.1/UA Active PSD Connections

2.1.4.1 FDP_APC_EXT.1.1/UA

The TSF shall route user data only to the interfaces selected by the user.

Evaluation activities are detailed below.

2.1.4.2 FDP_APC_EXT.1.2/UA

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

Evaluation activities are detailed below.

2.1.4.3 FDP_APC_EXT.1.3/UA

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

Evaluation activities are detailed below.

2.1.4.4 FDP_APC_EXT.1.4/UA

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

Application Note

This SFR is refined from the PSD PP for this PP-Module to include further restrictions for electrical signals. It is unlikely that this element can be satisfied unless user authentication peripheral device interfaces are electrically and logically isolated from the connected computer interfaces or through other methods.

If the TOE claims conformance to multiple PP-Modules, each PP-Module modifies this SFR in a different manner for the interfaces that are unique to that module. In this case, the ST author should reference this modification of the SFR as "FDP_APC_EXT.1/UA" for uniqueness. Note that all elements of FDP_APC_EXT.1 must be included in this iteration, not just the ones that are modified by this PP-Module.

Evaluation Activity

Isolation Document

There are no Isolation Document EAs for this component beyond what the PSD PP requires.

TSS

There are no TSS EAs for this component beyond what the PSD PP requires.

Guidance

There are no guidance EAs for this component beyond what the PSD PP requires.

Test

For tests that use the USB sniffer or USB analyzer software, the evaluator verifies whether traffic is sent or not sent by inspection of the passing USB transactions and ensuring they do not contain USB data payloads other than any expected traffic, as well as USB NAK transactions or system messages. To avoid clutter during USB traffic capture, the evaluator may filter NAK transactions and system messages.

Test Setup

For each of the below tests the evaluator shall perform the following test set up:

1. Configure the TOE and the operational environment in accordance with the operational guidance.

2. Connect a computer to each TOE UA computer interface and a display to each connected computer.

3. Open a real-time hardware information console and USB protocol analyzer software on each connected computer.

4. Ensure the user authentication application and driver for the authorized user authentication device used for testing is installed.

5. [Conditional: if "external" is selected in FDP_PDC_EXT.4.1, then:] connect an authorized user authentication device with a power LED and a connected DVM to each PSD UA peripheral device interface.

Test 1-UA: UA Switching methods

[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 the functionality of the TOE's UA switching methods.

While performing this test, ensure that switching is always initiated through express user action.

Step 1. Turn on the TOE and ensure computer #1 is selected.

Step 2: Verify that the real-time hardware information console on computer #1 indicates the presence of the user authentication device. [Conditional: if "external" is selected in FDP_PDC_EXT.4.1, then:] verify the UA device power LED is illuminated and the DVM reads between 4.75 and 5.25 VDC.

Step 3: Perform steps 4-6 for each connected computer.

Step 4: For each switching method selected in FDP_SWI_EXT.2.2, switch selected computers in accordance with the operational guidance.

Step 5: [Conditional: if "external" is selected in FDP_PDC_EXT.4.1, then:] verify that the LED for the UA device is not illuminated for at least one second while the DVM reads 0.5 VDC or less for at least one second.

Step 6: Verify that the real-time hardware console on the newly selected computer indicates the presence of the user authentication device. [Conditional: if "external" is selected in FDP_PDC_EXT.4.1, then:] verify the UA device power LED is illuminated and the DVM reads between 4.75 and 5.25 VDC.

Test 2-UA: Positive and Negative UA Data Flow Rules Testing

This test verifies correct data flows of a UA device during different power states of the selected computer.

Step 1: For each connected computer, connect a USB sniffer between it and the TOE or ensure the USB analyzer software is opened. Perform steps 2-14 with each connected computer as the selected computer.

Step 2: Connect an authentication session and verify that the session is connected on the selected computer and that the expected traffic is sent and captured using the USB analyzer.

Step 3: Remove the authentication element and verify the session is terminated on the selected computer.

Step 4: Insert the authentication element. Reconnect an authentication session, verify that the session is connected on the selected computer and that the expected traffic is sent and captured using the USB analyzer

[Conditional: Perform steps 5-6 if "external" is selected in FDP_PDC_EXT.4.1.]

Step 5: Disconnect the UA device and verify the session is terminated on the selected computer and that the real-time hardware console does not show the device and that no traffic is sent on the USB analyzer.

Step 6: Reconnect the UA device. Reconnect an authentication session, verify that the session is connected on the selected computer and that the expected traffic is sent and captured using the USB analyzer.

[Conditional: Perform steps 7-14 if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in

the PSD PP.]

Step 7: Verify that the real-time hardware console on each of the non-selected computers does not show the UA device and that no traffic is sent on the other USB analyzers.

Step 8: Switch to another connected computer. Verify that the authentication session on the previously selected computer is terminated, the real-time hardware console on each non-selected computer does not show the UA device, and that no traffic is sent on the other USB analyzers.

Step 9: Connect an authentication session and verify that the session is connected on the selected computer, the expected traffic is sent and captured using the USB analyzer, and no traffic is sent on the other USB analyzers.

Step 10: Switch to the originally selected computer. Verify the authentication session is still terminated, and reconnect an authentication session. Verify that no traffic is sent on the other USB analyzers.

Step 11: Disconnect and reconnect the TOE interface cables connected to the selected computer. Examine the USB analyzers on each of the non-selected computers and verify that no traffic is sent.

Step 12: Reconnect an authentication session and verify that no traffic is sent on the other USB analyzers. Reboot the selected computer. Examine the USB analyzers on each of the non-selected computers and verify that no traffic is sent.

Step 13: Reconnect an authentication session and verify that no traffic is sent on the other USB analyzers. Enter sleep or suspend mode in the selected computer. Examine the USB analyzers on each of the non-selected computers and verify that no traffic is sent.

Step 14: Exit sleep or suspend mode in the selected computer. Examine the USB analyzers on each of the non-selected computers and verify that no traffic is sent.

Step 15: Perform steps 16-17 when the TOE is off and then in a failure state.

Step 16: Verify that for each connected computer, no real-time hardware console shows the device and no traffic is sent on the USB analyzer.

Step 17: Verify the authentication session is terminated on the selected computer.

Test 3-UA: No Electrical Flow between Computer Interfaces.

[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 no electrical signals flow between connected computers when the TOE is powered on or off.

Perform this test for each TOE UA computer interface. Perform this test when the TOE is powered on and off.

Step 1: Disconnect the first computer and replace it with a switchable 5 volt power supply with a USB Type-B plug. Modulate the 5 volt supply 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 the non-selected USB analyzers.

[Conditional: Perform steps 2-4 if "external" is selected in FDP_PDC_EXT.4.1.]

Step 2: Disconnect the power supply and replace it with the computer.

Step 3: Connect the USB dummy load into the TOE UA peripheral device interface. Examine the USB analyzers on all non-selected computers and verify that no new USB traffic is captured.

Step 4: Disconnect the USB dummy load and replace it with a switchable 5 volt power supply with a USB Type-B plug. Modulate the 5 volt supply 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 the non-selected USB analyzers.

Test 4-UA: No Flow between Connected Computers over Time

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 UA computer port.

Note that instead of the session ID, the evaluator may substitute authentication element or other unique session identification characteristic detectable by the USB analyzer.

Step 1: Ensure only one computer is connected to the TOE and it is selected.

Step 2: Connect an authentication session and record the authentication session ID using the USB analyzer.

Step 3: Disconnect the first computer, connect the second computer to the same port, connect an authentication session, and record the authentication session ID in less time than the authentication device timeout.

Step 4: Verify that the authentication session ID is different.

Step 5: Disconnect the second computer, connect the first computer to the same port, reconnect the authentication session, and record the authentication session ID in less time than the authentication device timeout.

Step 6: Verify that the authentication session ID is different from the first two.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

NA

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

Test 1

1. Turn on the TOE and ensure computer #1 is selected.
2. Verify that the real-time hardware information console on computer #1 indicates the presence of the user authentication device. *[Conditional: if "external" is selected in FDP_PDC_EXT.4.1, then:]* verify the UA device power LED is illuminated and the DVM reads between 4.75 and 5.25 VDC.
3. Perform steps 4 - 6 for each connected computer.
4. For each switching method selected in FDP_SWI_EXT.2.2, switch selected computers in accordance with the operational guidance.
5. *[Conditional: if "external" is selected in FDP_PDC_EXT.4.1, then:]* verify that the LED for the UA device is not illuminated for at least one second while the DVM reads 0.5 VDC or less for at least one second.
6. Verify that the real-time hardware console on the newly selected computer indicates the presence of the user authentication device. *[Conditional: if "external" is selected in FDP_PDC_EXT.4.1, then:]* verify the UA device power LED is illuminated and the DVM reads between 4.75 and 5.25 VDC.

The evaluator confirmed that the functionality of the TOE's UA switching methods is successful.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 2

1. For each connected computer, connect a USB sniffer between it and the TOE or ensure the USB analyzer software is opened. Perform steps 2-14 with each connected computer as the selected computer.
2. Connect an authentication session and verify that the session is connected on the selected computer and that the expected traffic is sent and captured using the USB analyzer.
3. Remove the authentication element and verify the session is terminated on the selected computer.

4. Insert the authentication element. Reconnect an authentication session, verify that the session is connected on the selected computer and that the expected traffic is sent and captured using the USB analyzer.
5. *[Conditional: Perform steps 5-6 if “external” is selected in FDP_PDC_EXT.4.1.]* Disconnect the UA device and verify the session is terminated on the selected computer and that the real-time hardware console does not show the device and that no traffic is sent on the USB analyzer.
6. Reconnect the UA device. Reconnect an authentication session, verify that the session is connected on the selected computer and that the expected traffic is sent and captured using the USB analyzer.
7. [Conditional: Perform steps 7-14 if “switching can be initiated only through express user action” is selected in FDP_SWI_EXT.1.1 in the PSD PP.] Verify that the real-time hardware console on each of the non-selected computers does not show the UA device and that no traffic is sent on the other USB analyzers.
8. Switch to another connected computer. Verify that the authentication session on the previously selected computer is terminated, the real-time hardware console on each non-selected computer does not show the UA device, and that no traffic is sent on the other USB analyzers.
9. Connect an authentication session and verify that the session is connected on the selected computer, the expected traffic is sent and captured using the USB analyzer, and no traffic is sent on the other USB analyzers.
10. Switch to the originally selected computer. Verify the authentication session is still terminated and reconnect an authentication session. Verify that no traffic is sent on the other USB analyzers.
11. Disconnect and reconnect the TOE interface cables connected to the selected computer. Examine the USB analyzers on each of the non-selected computers and verify that no traffic is sent.
12. Reconnect an authentication session and verify that no traffic is sent on the other USB analyzers. Reboot the selected computer. Examine the USB analyzers on each of the non-selected computers and verify that no traffic is sent.
13. Reconnect an authentication session and verify that no traffic is sent on the other USB analyzers. Enter sleep or suspend mode in the selected computer. Examine the USB analyzers on each of the non-selected computers and verify that no traffic is sent.
14. Exit sleep or suspend mode in the selected computer. Examine the USB analyzers on each of the non-selected computers and verify that no traffic is sent.
15. Perform steps 16-17 when the TOE is off and then in a failure state.
16. Verify that for each connected computer, no real-time hardware console shows the device and no traffic is sent on the USB analyzer.
17. Verify the authentication session is terminated on the selected computer.

The evaluator confirmed correct data flows of a UA device during different power states of the selected computer**.**

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 3

1. [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 verified no electrical signals flow between connected computers when the TOE is powered on or off. Perform this test for each TOE UA computer interface.

Perform this test when the TOE is powered on and off. Disconnect the first computer and replace it with a switchable 5-volt power supply with a USB Type-B plug. Modulate the 5-volt supply 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 the non-selected USB analyzers.

2. *[Conditional: Perform steps 2-4 if "external" is selected in FDP_PDC_EXT.4.1.]* Disconnect the power supply and replace it with the computer.
3. Connect the USB dummy load into the TOE UA peripheral device interface. Examine the USB analyzers on all non-selected computers and verify that no new USB traffic is captured.
4. Disconnect the USB dummy load and replace it with a switchable 5-volt power supply with a USB Type-B plug. Modulate the 5 volts supply 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 the non-selected USB analyzers.

The evaluator confirmed that no electric signals flow between connected computers when the TOE is powered on or off.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 4

1. Ensure only one computer is connected to the TOE and it is selected.
2. Connect an authentication session and record the authentication session ID using the USB analyzer.
3. Disconnect the first computer, connect the second computer to the same port, connect an authentication session, and record the authentication session ID in less time than the authentication device timeout.
4. Verify that the authentication session ID is different.
5. Disconnect the second computer, connect the first computer to the same port, reconnect the authentication session, and record the authentication session ID in less time than the authentication device timeout.
6. Verify that the authentication session ID is different from the first two.

The evaluator confirmed that the TOE does not send data to different computers connected to the same interface at different times.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

2.1.5 FDP_APC_EXT.1/VI Active PSD Connections

2.1.5.1 FDP_APC_EXT.1.1/VI

The TSF shall route user data only from the interfaces selected by the user.

Evaluation activities are detailed below.

2.1.5.2 FDP_APC_EXT.1.2/VI

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

Evaluation activities are detailed below.

2.1.5.3 FDP_APC_EXT.1.3/VI

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

Evaluation activities are detailed below.

2.1.5.4 FDP_APC_EXT.1.4/VI

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

Application Note

This SFR is refined from the PSD PP for this PP-Module to include further restrictions for electrical signals. It is unlikely that this element can be satisfied unless video/display peripheral device interfaces are electrically and logically isolated from the connected computer interfaces or through other methods.

If the TOE claims conformance to multiple PP-Modules, each PP-Module modifies this SFR in a different manner for the interfaces that are unique to that module. In this case, the ST author should reference this modification of the SFR as "FDP_APC_EXT.1/VI" for uniqueness. Note that all elements of FDP_APC_EXT.1 must be included in this iteration, not just the ones that are modified by this PP-Module.

Evaluation Activity

Isolation Document

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).

TSS

There are no guidance EAs for this component beyond what the PSD PP requires.

[Note to evaluator: This was copied directly from mod_vi_v1.0-sd.pdf. It is unclear whether NIAP intended no TSS EAs or whether the TSS EAs are missing.]

Guidance

There are no guidance EAs for this component beyond what the PSD PP requires.

Test

The evaluator shall perform the following tests:

Test 1-VI: Video Source Selection and Identification, TOE Off and Failure States

This test verifies the TOE switching function operates properly and will stop the video output display when in an OFF or FAILURE state.

Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance.

Step 2: Play a different video with embedded audio on a number of computers for each TOE computer video interface.

Step 3: Connect each computer to a TOE computer video interface.

Step 4: Connect a display to each TOE display interface.

Step 5: Turn on the TOE.

Step 6: For each connected computer, ensure it is selected and verify that the video and its accompanying audio from the selected computer(s) are received on the proper display(s).

Step 7: [Conditional: if claims Combiner Use Case then] verify that video generated by the TOE has clear identification marking or text to properly identify the source computer shown. ***Note: TD0539 applied***

Step 8: Turn off the TOE and verify that no video appears on any connected display.

Step 9: Power on the TOE and cause the TOE to enter a failure state. Verify that the TOE provides the user with a visual indication of failure and that no usable video appears on any connected display.

Step 10: Repeat steps 3 to 9 for each unique display protocol and port type supported by the TOE.

Test 2-VI: Computer Video Interface Isolation

[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 that the TOE does not transfer data to any non-selected computer video interface.

Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect only the first computer interface cable to one computer. Turn on the TOE.

Step 2: Switch the TOE primary display to computer #1.

Step 3: Observe the primary display to verify that the selected computer is the one that is shown.

Step 4: Remove the non-selected computer video interface cables from the TOE and connect the oscilloscope probe to the TOE #2 computer video interface to verify that no SYNC signal is passed through the TOE. Based on the connection interface protocol, this is performed as follows:

1. Video Graphics Array (VGA) – single ended probe on pins 13 and then 14;

2. High-Definition Multimedia Interface (HDMI) – connect pin 19 to a 3.3V power supply via a 100 Ohm resistor to provide Hot Plug Detect (HPD) signal; Check for signals - differential probe between pins 10 (+) and 12 (-);

3. Digital Visual Interface (DVI)-I – connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - single ended probe on pins 8 and C4. Differential probe between pins 23 (+) and 24 (-);

4. DVI-D - connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 23 (+) and 24 (-);

5. DisplayPort - connect pin 18 to a 3.3V power supply via 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 3 (-) and 1 (+) and between 10 (-) and 12 (+);

6. USB Type-C with DisplayPort as Alternate Function – connect pin A8 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals – Differential probe between pins A2 and A3, A10 and A11; B2 and B3, and B10 and B11.

Step 5: Repeat steps 3 and 4 while selecting other TOE connected computers. Verify that no SYNC signal is present.

Step 6: Repeat steps 3 to 5 with the TOE unpowered. Verify that no SYNC signal is present.

Step 7: With the probe connected to the TOE computer #2 video interface, disconnect / reconnect the computer #1 video cable. Power up the TOE and select computer #1. Attempt to detect the change in the oscilloscope at each one of the TOE #2 computer video interface pins. No changes shall be detected.

Step 8: Repeat step 7 for each one of the other TOE computer video interfaces.

Step 9: Repeat steps 7 and 8, but instead of disconnecting / reconnecting the computer, disconnect and reconnect the display.

Step 10: Repeat steps 7 and 8, but instead of disconnecting / reconnecting the computer, reboot the selected computer.

Step 11: Repeat steps 2 to 10 with each connected computer.

Step 12: [Conditional: if "multiple connected displays" is selected in FDP_CDS_EXT.1.1 then] repeat steps 3 to 10 with each other display connected to the TOE.

Step 13: Repeat this test for each unique display protocol and port type supported by the TOE.

Test 3-VI - Unauthorized Sub-protocols

Note that in the following steps only native video protocol cables shall be used. No conversion from other video protocols is allowed *in these tests except as directed in FDP_IPC_EXT.1.1.*

This test verifies that unauthorized sub-protocols are blocked.

Perform this test for each of the selections in FDP_PDC_EXT.3.1/VI and FDP_IPC_EXT.1.1.

In the following steps the evaluator shall establish a verified test setup that passes video signals across the TOE.

Step 1: Connect at least one computer with a native video protocol output to the TOE computer #1 video input interface.

Step 2: Connect at least one display with native video protocol to the TOE display output.

Step 3: Power up the TOE and ensure the connected computer is selected.

Step 4: Verify that the video image is visible and stable on the user display.

In the following steps the evaluator shall verify that the test setup properly blocks the unauthorized video sub-protocol traffic.

Step 5: Open the Monitor Control Command Set (MCCS) control console program on the computer and attempt to change the display contrast and brightness. Verify that the display does not change its contrast and brightness accordingly.

Step 6: Disconnect the video cable connecting the display and the TOE and connect the display directly to the computer. Verify that the video image is visible and stable on the user display. ***Note: TD0514 applied***

Step 7: Attempt to change the display contrast and brightness. Verify that the display does change its contrast and brightness accordingly.

Step 8: Connect the following testing device based on the display video protocol being tested at the peripheral display interface:

1. *DisplayPort – DisplayPort AUX channel analyzer in series between the display and the TOE*
2. *HDMI– HDMI sink test device*
3. *USB Type-C with DisplayPort as Alternate Function – USB sniffer in series between the display and the TOE*
4. *VGA – VGA sink test device*
5. *DVI-I/DVI-D – DVI sink test device*

Note: TD0584 applied

Step 9: Attempt to change the display contrast and brightness. Verify that the testing device does not capture any MCCS commands.

Step 10: Replace the computer with a source generator for each selected protocol at the computer video interface. If DVI-I or DVI-D is selected, use an HDMI source generator.

Step 11: Run an EDID write transaction at the generator and verify in the testing device that no EDID traffic is captured.

Step 12: [Conditional, if DisplayPort, DVI-D, DVI-I, HDMI, or USB Type-C is the selected protocol being tested at the computer video interface, then] run Consumer Electronics Control (CEC) and High-bandwidth Digital Content Protection (HDCP) tests or commands at the generator and verify in the testing device that no CEC or HDCP traffic is captured.

Step 13: [Conditional, if DVI-D, DVI-I, or HDMI is the selected protocol being tested at the computer video interface, then] run Audio Return Channel (ARC), HDMI Ethernet and Audio Return Channel (HEAC), and HDMI Ethernet Channel (HEC) tests or commands at the generator and verify in the testing device that no ARC, HEAC, or HEC traffic is captured.

Step 14: [Conditional: If "[HDMI] protocol" is selected in FDP_IPC_EXT.1.2, then] perform steps 15 and 16 for both pin 13 (CEC) and 14 (UTILITY).

Step 15: Turn off the TOE. Use a multi-meter to measure the resistance-to-ground of the pin at the TOE HDMI peripheral interface and verify it is greater than 2 Mega-ohms.

Step 16: Attach a single ended oscilloscope probe between the pin and the ground, turn on the TOE, and verify that no changes between 0.0v and 0.2v and between 3.0v and 3.3v are detected.

Step 17: [Conditional: if VGA is not the selected protocol being tested, then] disconnect all devices. Connect the display to a TOE computer video interface and the oscilloscope to the TOE display interface in order to verify that no HPD signal is passed by *measuring a signal voltage of less than 1.0V. Based on the selected protocol being tested, this is performed as follows:*

1. *HDMI – connect scope to pin 19 and verify no HPD signal is detected;*
2. *DVI-D/DVI-I – connect scope to pin 16 and verify no HPD signal is detected;*
3. *DisplayPort - connect scope to pin 18 and verify no HPD signal is detected;*
4. *USB Type-C with DisplayPort as Alternate Function – connect scope to pin A8 and B8 and verify no HPD signal is detected.*

Step 18: Repeat this test for each of the selections in FDP_PDC_EXT.3.1/VI and FDP_IPC_EXT.1.2.

Test 4-VI - Video and EDID Channel Unidirectional Rule

This test verifies that the TOE video path is unidirectional from the computer video interface to the display interface with the exception of EDID, which may be read from the display once at power up and then may be read by the connected computers. The evaluator should have at least two high-resolution displays and one low-resolution display for each TOE-supported video protocol.

In the following steps the evaluator should attempt to read display EDID after the TOE completed its self-test / power up. The TOE should not read the new display EDID.

Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect a computer and a high-resolution display to the TOE.

Step 2: Ensure the TOE is on, computer #1 is selected, and verify that the display shows video from computer #1 as expected.

Step 3: Turn off the TOE. Disconnect the user display from the TOE.

Step 4: Connect the low-resolution display to the TOE and turn on the TOE. After the video is shown on the display, turn off the TOE and disconnect the low-resolution display. ***Note: TD0506 applied***

Step 5: Turn on the TOE. After the TOE has completed the self-test, connect the second high-resolution display of a different model to the TOE. The TOE may fail to generate video on the user display (i.e., no EDID is read at the TOE power up). If the display is showing video, then run the EDID reading and parsing software on computer #1 and check that there is no active EDID (i.e., the computer is using a default generic display or reading older display settings from the registry). ***Note: TD0506 applied***

In the following steps the evaluator shall validate that the TOE video path is unidirectional from the computer video interface to the display interface.

Step 6: Perform steps 7-11 for each TOE computer video interface.

Step 7: Power off the TOE and disconnect the computer #1 video output and the display. Connect the display cable to the TOE computer #1 video interface. Connect the computer #1 video cable to the TOE display interface. This configuration will attempt to force video data through the TOE in the reverse direction.

Step 8: Power up the TOE again.

Step 9: Check that the video is not visible in the display.

Step 10: Perform steps 11 while the TOE is powered on and powered off.

Step 11: Remove the display cable from the TOE and connect the oscilloscope to verify that no SYNC signal is passed through the TOE. Based on the video protocols supported, this is performed as follows:

1. *VGA – single ended probe on pins 13 and 14;*
2. *HDMI – connect pin 19 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - differential probe between pins 10 (+) and 12 (-);*
3. *DVI-I – connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - single ended probe on pins 8 and C4. Differential probe between pins 23 (+) and 24 (-);*
4. *DVI-D - connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 23 (+) and 24 (-);*
5. *DisplayPort - connect pin 18 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 3 (-) and 1 (+) and between 10 (-) and 12 (+);*
6. *USB Type-C with DisplayPort as Alternate Function – connect pin A8 to a 3.3V power supply via a 100 Ohm resistor to provide*

HPD signal; Check for signals – Differential probe between pins A2 and A3, A10 and A11; B2 and B3, and B10 and B11.

Test 5-VI – No Flow between Connected Computers over Time

This test verifies that the TOE does not send data to different computers connected to the same TOE video interface over time. Repeat this test for each TOE Video port.

Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Run EDID reading and parsing software on two computers and connect a display to the TOE.

Step 2: Connect computer #1 to the TOE, ensure the TOE is on, computer #1 is selected, no other computers are connected, and verify that the display shows video from computer #1 as expected.

Step 3: Capture the TOE EDID content in the software on computer #1 and save as a file with a name that indicates capture time.

Step 4: Disconnect computer #1 and connect an I2C programmer to the same port. Attempt to write the characters "FFFF" over the entire EDID address range.

Step 5: Disconnect the I2C programmer, reconnect computer #1 to the same port, and repeat step 3.

Step 6: Reboot the TOE and repeat step 3.

Step 7: Turn off the TOE and repeat step 3.

Step 8. Restart the TOE and repeat step 3.

Step 9: Disconnect computer #1 and repeat steps 2 to 8 with computer #2 on the same port.

Step 10: Repeat steps 2 to 9 for a total of 20 EDID file captures.

Step 11: Collect all 20 captured EDID files, compare them bit-by-bit, and verify that they are identical excluding null captures recorded in Step 7. ***Note: TD0584 applied***

Isolation Document Evaluator Assessment:

[Isol] has 2 figures, (figure 1 and figure2) that illustrate all possible data flows. There follows a table, Table 1 Data Flow, that gives an explanation of all data flows. Figures 3, 4 ,5, 6, 7 and 9 which characterize the data flows for various parts of the TOE (i.e. combiners, switches, etc.) are part of the isolation justification and indicate the methods used to maintain the data separation. Section 2.3, Figure 3 of [Isol] gives an explanation of all data flow isolation. Section 2.4 discusses power isolation. Section 3 describes the isolation enforcement policy for various aspects of the TOE. Figure 8 shows the physical characteristics. A complete analysis of the Isolation document is found in the file CFG_PSD-AO-KM-UA-VI - Annex D HSL Isolation Documentation assessment.doc.

TSS Evaluator Assessment:

NA

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

Test 1

1. Configure the TOE and the Operational Environment in accordance with the operational guidance.
2. Play a different video with embedded audio on a number of computers for each TOE computer video interface.
3. Connect each computer to a TOE computer video interface.
4. Connect a display to each TOE display interface.
5. Turn on the TOE.

6. For each connected computer, ensure it is selected and verify that the video and its accompanying audio from the selected computer(s) are received on the proper display(s).
7. *[Conditional: if the TOE claims the Combiner Use Case then]* verify that video generated by the TOE has clear identification marking or text to properly identify the source computer shown. Note:TD0539 applied
8. Turn off the TOE and verify that no video appears on any connected display.
9. Power on the TOE and cause the TOE to enter a failure state. Verify that the TOE provides the user with a visual indication of failure and that no usable video appears on any connected display.
10. Repeat steps 3 to 9 for each unique display protocol and port type supported by the TOE.

The evaluator confirmed that the TOE switching function operates properly and will stop the video output display when in an OFF or FAILURE state.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 2

1. Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect only the first computer interface cable to one computer. Turn on the TOE.
2. Switch the TOE primary display to computer #1.
3. Observe the primary display to verify that the selected computer is the one that is shown.
4. Remove the non-selected computer video interface cables from the TOE and connect the oscilloscope probe to the TOE #2 computer video interface to verify that no SYNC signal is passed through the TOE. Based on the connection interface protocol, this is performed as follows:

   High-Definition Multimedia Interface (HDMI) – connect pin 19 to a 3.3V power supply via a 100 Ohm resistor to provide Hot Plug Detect (HPD) signal; Check for signals - differential probe between pins 10 (+) and 12 (-);

   DVI-D - connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 23 (+) and 24 (-);
   DisplayPort - connect pin 18 to a 3.3V power supply via 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 3 (-) and 1 (+) and between 10 (-) and 12 (+);

5. Repeat steps 3 and 4 while selecting other TOE connected computers. Verify that no SYNC signal is present.
6. Repeat steps 3 to 5 with the TOE unpowered. Verify that no SYNC signal is present.
7. With the probe connected to the TOE computer #2 video interface, disconnect / reconnect the computer #1 video cable. Power up the TOE and select computer #1. Attempt to detect the change in the oscilloscope at each one of the TOE #2 computer video interface pins. No changes shall be detected.
8. Repeat step 7 for each one of the other TOE computer video interfaces.
9. Repeat steps 7 and 8, but instead of disconnecting / reconnecting the computer, disconnect and reconnect the display.
10. Repeat steps 7 and 8, but instead of disconnecting / reconnecting the computer, reboot the selected computer.
11. Repeat steps 2 to 10 with each connected computer.

12. [*Conditional: if "multiple connected displays" is selected in FDP_CDS_EXT.1.1 then]* repeat steps 3 to 10 with each other display connected to the TOE.
13. Repeat this test for each unique display protocol and port type supported by the TOE.

The evaluator confirmed that the TOE does not transfer data to any non-selected computer video interface.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 3

1. Connect at least one computer with a native video protocol output to the TOE computer #1 video input interface.
2. Connect at least one display with native video protocol to the TOE display output.
3. Power up the TOE and ensure the connected computer is selected.
4. Power up the TOE and ensure the connected computer is selected.
5. Open the Monitor Control Command Set (MCCS) control console program on the computer and attempt to change the display contrast and brightness. Verify that the display does not change its contrast and brightness accordingly.
6. Disconnect the video cable connecting the display and the TOE and connect the display directly to the computer. Verify that the video image is visible and stable on the user display. Note: TD0514 applied
7. Attempt to change the display contrast and brightness. Verify that the display does change its contrast and brightness accordingly.
8. Connect the following testing device based on the display video protocol being tested at the peripheral display interface: (Note: TD0584 applied)
   DisplayPort – DisplayPort AUX channel analyzer in series between the display and the TOE
   HDMI – HDMI sink test device

9. Attempt to change the display contrast and brightness. Verify that the testing device does not capture any MCCS commands.
10. Replace the computer with a source generator for each selected protocol at the computer video interface. If DVI-I or DVI-D is selected, use an HDMI source generator.
11. Run an EDID write transaction at the generator and verify in the testing device that no EDID traffic is captured.
12. *[Conditional, if DisplayPort, DVI-D, DVI-I, HDMI, or USB Type-C is the selected protocol being tested at the computer video interface, then]* run Consumer Electronics Control (CEC) and High-bandwidth Digital Content Protection (HDCP) tests or commands at the generator and verify in the testing device that no CEC or HDCP traffic is captured.
13. *[Conditional, if DVI-D, DVI-I, or HDMI is the selected protocol being tested at the computer video interface, then]* run Audio Return Channel (ARC), HDMI Ethernet and Audio Return Channel (HEAC), and HDMI Ethernet Channel (HEC) tests or commands at the generator and verify in the testing device that no ARC, HEAC, or HEC traffic is captured.
14. *[Conditional: If "[HDMI] protocol" is selected in FDP_IPC_EXT.1.2, then]* perform steps 15 and 16 for both pin 13 (CEC) and 14 (UTILITY).

15. Turn off the TOE. Use a multi-meter to measure the resistance-to-ground of the pin at the TOE HDMI peripheral interface and verify it is greater than 2 Mega-ohms.
16. Attach a single ended oscilloscope probe between the pin and the ground, turn on the TOE, and verify that no changes between 0.0v and 0.2v and between 3.0v and 3.3v are detected.
17. *[Conditional: if VGA is not the selected protocol being tested, then]* disconnect all devices. Connect the display to a TOE computer video interface and the oscilloscope to the TOE display interface in order to verify that no HPD signal is passed by measuring a signal voltage of less than 1.0V. Based on the selected protocol being tested, this is performed as follows:
    1. HDMI – connect scope to pin 19 and verify no HPD signal is detected;
    3. DisplayPort - connect scope to pin 18 and verify no HPD signal is detected;
    4. USB Type-C with DisplayPort as Alternate Function – connect scope to pin A8 and B8 and verify no HPD signal is detected.
18. Repeat this test for each of the selections in FDP_PDC_EXT.3.1/VI and FDP_IPC_EXT.1.2

The evaluator has confirmed that the TOE successfully blocks unauthorized sub-protocols.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 4

1. Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect a computer and a high-resolution display to the TOE.
2. Ensure the TOE is on, computer #1 is selected, and verify that the display shows video from computer #1 as expected.
3. Turn off the TOE. Disconnect the user display from the TOE.
4. Connect the low-resolution display to the TOE and turn on the TOE. After the video is shown on the display, turn off the TOE and disconnect the low-resolution display. Note: TD0506 applied
5. Turn on the TOE. After the TOE has completed the self-test, connect the second high-resolution display of a different model to the TOE. The TOE may fail to generate video on the user display (i.e., no EDID is read at the TOE power up). If the display is showing video, then run the EDID reading and parsing software on computer #1 and check that there is no active EDID (i.e., the computer is using a default generic display or reading older display settings from the registry). Note: TD0506 applied
6. Perform steps 7-11 for each TOE computer video interface.
7. Power off the TOE and disconnect the computer #1 video output and the display. Connect the display cable to the TOE computer #1 video interface. Connect the computer #1 video cable to the TOE display interface. This configuration will attempt to force video data through the TOE in the reverse direction.
8. Power up the TOE again.
9. Check that the video is not visible in the display.
10. Perform steps 11 while the TOE is powered on and powered off.
11. Remove the display cable from the TOE and connect the oscilloscope to verify that no SYNC signal is passed through the TOE. Based on the video protocols supported, this is performed as follows:
    HDMI – connect pin 19 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - differential probe between pins 10 (+) and 12 (-);

    DisplayPort - connect pin 18 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 3 (-) and 1 (+) and between 10 (-) and 12 (+);

The evaluator confirmed the TOE video path is unidirectional from the computer video interface to the display interface except for EDID.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 5

1. Configure the TOE and the Operational Environment in accordance with the operational guidance. Run EDID reading and parsing software on two computers and connect a display to the TOE.
2. Connect computer #1 to the TOE, ensure the TOE is on, computer #1 is selected, no other computers are connected, and verify that the display shows video from computer #1 as expected.
3. Capture the TOE EDID content in the software on computer #1 and save as a file with a name that indicates capture time.
4. Disconnect computer #1 and connect an I2C programmer to the same port. Attempt to write the characters “FFFF” over the entire EDID address range.
5. Disconnect the I2C programmer, reconnect computer #1 to the same port, and repeat step 3.
6. Reboot the TOE and repeat step 3.
7. Turn off the TOE and repeat step 3.
8. Restart the TOE and repeat step 3.
9. Disconnect computer #1 and repeat steps 2 to 8 with computer #2 on the same port.
10. Repeat steps 2 to 9 for a total of 20 EDID file captures.
11. Collect all 20 captured EDID files, compare them bit-by-bit, and verify that they are identical excluding null captures recorded in Step 7. Note: TD0584 applied

The evaluator confirmed that that the TOE does not send data to different computers connected to the same TOE video interface over time.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

2.1.6 FDP_FIL_EXT.1/UA Device Filtering (User Authentication Devices)

2.1.6.1 FDP_FIL_EXT.1.1/UA

The TSF shall have [selection: configurable, fixed] device filtering for [user authentication device] interfaces.

Application Note:

The ST author must make the selection for the device which the TOE has: configurable, fixed or both.

2.1.6.2 FDP_FIL_EXT.1.2/UA

The TSF shall consider all [PSD UA] blacklisted devices as unauthorized devices for [user authentication device] interfaces in peripheral device connections.

2.1.6.3 FDP_FIL_EXT.1.3/UA

The TSF shall consider all [PSD UA] whitelisted devices as authorized devices for [user authentication device] interfaces in peripheral device connections only if they are not on the [PSD UA] blacklist or otherwise unauthorized.

Application Note

The ST author must make the selections for the device which the TOE has: configurable or fixed or both; and keyboard or mouse or both.

Evaluation Activity

Note: if "configurable" is selected in FDP_FIL_EXT.1.1/UA, the evaluator shall perform these activities in conjunction with the FMT_MOF.1 and FMT_SMF.1 evaluation activities specified in the PSD PP because configuring the device filtration rules involves use of the TOE's management functionality.

Isolation Document

There are no Isolation Document activities for this SFR.

TSS

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/UA, then:] The evaluator shall examine the TSS and verify that it describes the process of configuring the TOE for whitelisting and blacklisting UA peripheral devices, including information on how this function is restricted to administrators.

Guidance

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

Test

Test 1

Perform the test steps in FDP_PDC_EXT.1 with all devices on the PSD UA blacklist and verify that they are rejected as expected.

Test 2

[Conditional: Perform this only if "configurable" is selected in FDP_FIL_EXT.1.1/UA]

In the following steps the evaluator shall verify that whitelisted and blacklisted devices are treated correctly.

Step 1: Configure the TOE UA CDF to whitelist an authorized user authentication device, connect it to the TOE UA peripheral device interface, and verify that the device is accepted through real-time device console and USB sniffer capture.

Step 2: Configure the TOE UA CDF to blacklist the device and verify that the device is rejected through real-time device console and USB sniffer capture.

Step 3: Attempt to configure the TOE UA CDF to both whitelist and blacklist the device and verify that the device is rejected through real-time device console and USB sniffer capture.

Test 3

[Conditional – Perform this only if "fixed" is selected in FDP_FIL_EXT.1.1/UA]

The evaluator shall examine the PSD UA whitelist and verify that all devices are authorized devices.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

The devices have configurable filtering for UA. Section 9.2.4 states. "An authorized administrator can configure the TOE to whitelist or blacklist particular device types for use on this port. The administrator must first log into the TOE administrative console. Using this interface, any USB 1.1, 2.0 or 3.0 compatible device can be whitelisted or blacklisted based on one or more of the following:

- USB Class
- USB Sub-class
- USB Protocol
- USB device ID
- USB Vendor ID
- USB Serial number"

Guidance Evaluator Assessment:

The filtering is configurable. The whitelist contains all authorized devices and blacklist contains the unauthorized devices. The [19959], [19961], and [20601] discuss the authorized and unauthorized devices.

Test Evaluator Assessment:

Test 1

1. Ensure the TOE is powered off and connected to a computer. Run USB analyzer software and open the real-time hardware console on the connected computer and connect a USB sniffer to the unauthorized device.
2. Attempt to connect the unauthorized device via the USB sniffer to the TOE UA peripheral interface.
3. Power on the TOE. Verify the device is rejected.
4. Ensure the unauthorized device is disconnected from the TOE UA peripheral interface, then attempt to connect it again.
5. Verify the device is rejected.
6. Repeat steps 1-5 with a USB hub connected between the USB device and the USB sniffer and observe that the results are identical.

The evaluator confirmed that all devices on the PSD UA blacklist are rejected as expected.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 2

1. Configure the TOE UA CDF to whitelist an authorized user authentication device, connect it to the TOE UA peripheral device interface, and verify that the device is accepted through real-time device console and USB sniffer capture.
2. Configure the TOE UA CDF to blacklist the device and verify that the device is rejected through real-time device console and USB sniffer capture.
3. Attempt to configure the TOE UA CDF to both whitelist and blacklist the device and verify that the device is rejected through real-time device console and USB sniffer capture.

The evaluator confirmed that whitelisted and blacklisted devices are treated correctly.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 3

NA “Configurable” has been selected, and therefore this evaluation activity is not applicable.

2.1.7 FDP_PDC_EXT.1 Peripheral Device Connection

Note: The inclusion of [MOD_VI_V1.0] triggers additions to the Peripheral Device Connections Policy (see Appendix E) associated with this SFR and additional Evaluation Activities.

2.1.7.1 FDP_PDC_EXT.1.1

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

Evaluation activities are detailed below.

2.1.7.2 FDP_PDC_EXT.1.2

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

Evaluation activities are detailed below.

2.1.7.3 FDP_PDC_EXT.1.3

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

Evaluation activities are detailed below.

2.1.7.4 FDP_PDC_EXT.1.4

The TOE shall not have wireless interfaces.

Evaluation activities are detailed below.

2.1.7.5 FDP_PDC_EXT.1.5

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

Application Note

The Peripheral Device Connections section is in Appendix E of both the PSD PP and this PP-Module. Keyboard and mouse peripheral device ports may be specific to only one type or interchangeable between them.

The TSF may elect to enforce rejection of unauthorized devices connected to the PSD through a USB hub by considering USB hubs as unauthorized devices, even though USB hubs are authorized devices. The TSF may elect to enforce rejection of unauthorized non-HID device classes of a composite device connected to a TOE KM peripheral interface by considering composite devices with non-HID device classes as unauthorized devices, even though the HID device classes are authorized.

[UA] The TSF may elect to enforce rejection of unauthorized devices connected to the PSD through a USB hub by considering USB hubs as unauthorized devices, even though USB hubs are authorized devices. If "internal" is the only selection made in FDP_PDC_EXT.4.1, then the TSF does not have to support USB as an authorized interface unless the KM PP-Module is also claimed by the ST author.

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this component.

TSS

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).

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.

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.

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.

Guidance

The evaluator shall verify that the operational user guidance provides clear direction for the connection of computers and peripheral devices to the TOE.

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.

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.

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.

[KM] 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.

[UA] 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.

[VI] 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.

Test

Test 1: The evaluator shall check the TOE and its supplied cables and accessories to ensure that there are no external wired interfaces other than computer interfaces, peripheral device interfaces, and power interfaces.

Test 2: The evaluator shall check the TOE for radio frequency certification information to ensure that the TOE does not support wireless interfaces.

Test 3: 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.

Step 1: Ensure the TOE is powered off. Open a real-time hardware information console on the connected computer.

Step 2: Attempt to connect a USB mass storage device to the TOE peripheral interface.

Step 3: Power on the TOE. Verify the device is rejected.

Step 4: Ensure the USB mass storage device is disconnected, and then attempt to connect it to the TOE peripheral interface again.

Step 5: Verify the device is rejected.

Step 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.

Step 7: Power on the TOE. Verify the device is rejected.

Step 8: Ensure the USB hub is disconnected, and then attempt to connect it to the TOE peripheral interface again.

Step 9: Verify the device is rejected.

Step 10: Power off the TOE. Attempt to connect any Personal System/2 (PS/2) device directly to the TOE peripheral interface.

Step 11: Power on the TOE. Verify the device is rejected.

Step 12: Ensure the PS/2 device is disconnected, and then attempt to connect it directly to the TOE peripheral interface again.

Step 13: Verify the device is rejected.

Test 1-AO

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 or an immediate cessation of traffic following device detection or enumeration, or incompatibility of the device interface with the peripheral interface.

Step 1: Ensure the TOE is powered off and audio analyzer software is running on the connected computer.

Step 2: Connect an analog microphone to the TOE analog audio output peripheral interface.

Step 3: Power on the TOE, speak loudly into the microphone from approximately one-inch distance, and verify no audio is present in the audio analyzer software.

Step 4: Disconnect the microphone and reconnect it to the TOE peripheral interface.

Step 5: Speak loudly into the microphone from approximately one-inch distance, and verify no audio is present in the audio analyzer software.

Test 1-KM

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 1-6 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

Step 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.

Step 2: Attempt to connect the unauthorized device to the USB sniffer.

Step 3: Power on the TOE. Verify the device is rejected.

Step 4: Ensure the unauthorized device is disconnected from the USB sniffer, then attempt to connect it to the USB sniffer again.

Step 5: Verify the device is rejected.

Step 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.

Step 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.

Test 2-KM

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).

Step 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.

Step 2: Ensure the TOE is powered off.

Step 3: Connect the authorized device to the TOE peripheral interface.

Step 4: Power on the TOE. Verify the TOE user indication described in the operational user guidance is not present.

Step 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.

Step 6: Disconnect the authorized device, and then reconnect it to the TOE KM peripheral device interface.

Step 7: Verify the TOE user indication described in the operational user guidance is not present.

Step 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.

Test 1-UA

[Conditional: Perform this test if "external" is selected in FDP_PDC_EXT.4.1]

This test verifies 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).

Perform this test for an unauthorized device presenting itself as a composite device, a USB camera, a USB audio headset, a USB printer, a USB keyboard, a USB wireless dongle, and any device listed on the PSD UA blacklist.

Repeat this for each user authentication TOE peripheral interface.

Step 1: Ensure the TOE is powered off and connected to a computer. Run USB analyzer software and open the real-time hardware console on the connected computer, and connect a USB sniffer to the unauthorized device.

Step 2: Attempt to connect the unauthorized device via the USB sniffer to the TOE UA peripheral interface.

Step 3: Power on the TOE. Verify the device is rejected.

Step 4: Ensure the unauthorized device is disconnected from the TOE UA peripheral interface, then attempt to connect it again.

Step 5: Verify the device is rejected.

Step 6: Repeat steps 1-5 with a USB hub connected between the USB device and the USB sniffer and observe that the results are identical

Test 2-UA: Authorized Device Acceptance

[Conditional: Perform this test if "external" is selected in FDP_PDC_EXT.4.1]

This test verifies that the TOE ports do not reject authorized devices and devices with authorized protocols as per the Peripheral Device Connection Policy.

Perform this test for a USB device identified as User Authentication and any device listed on the PSD UA whitelist:

Step 1: Ensure the TOE is powered off.

Step 2: Connect the authorized device to the TOE peripheral interface.

Step 3: Power on the TOE. Verify the TOE user indication described in the operational user guidance is not present.

Step 4: Ensure the connected computer is selected and attempt to connect an authentication session. Verify that the authentication session is successfully connected on the connected computer.

Step 5: Disconnect the authorized device, then reconnect it to the TOE peripheral interface.

Step 6: Verify the TOE user indication described in the operational user guidance is not present.

Step 7: Attempt to start an authentication session. Verify that the authentication session begins on the connected computer.

Test 1-VI

The evaluator shall verify that the TOE ports do not reject authorized devices and devices with authorized protocols as per the Peripheral Device Connections appendix in MOD_VI_V1.0.

Repeat this test for each of the selected protocols in FDP_PDC_EXT.3.1/VI:

Step 1: Connect the authorized device with an authorized protocol directly to a computer. Display any image on the device. Disconnect the device from the computer.

Step 2: Configure the TOE and the Operational Environment in accordance with the operational guidance.

Step 3: Ensure the TOE is powered off.

Step 4: Connect the authorized device with an authorized protocol to the TOE peripheral interface.

Step 5: Power on the TOE and verify the TOE user indication described in the operational user guidance is not present.

Step 6: Ensure the connected computer is selected and verify that the device displays the same image as in step 1.

Step 7: Disconnect the authorized device, then reconnect it to the TOE peripheral interface.

Step 8: Verify the TOE user indication described in the operational user guidance is not present.

Step 9: Verify that the device displays the same image as in step 1 and 6.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

There are no wireless peripherals allowed in this configuration. The TSS section 9.2.2.3 states "The TOE does not support a wireless connection to a mouse, keyboard or USB hub." Section 9.2.3.1 states "The TOE does not support a wireless connection to a video display." Section 9.2.4.1 states "The TOE does not support a wireless connection to an authentication device." Section 9.2.5.1 states "The TOE does not support a wireless connection to an audio output device." The TSS describes all interfaces between the computers and the peripheral devices in sections 9.1 to 9.5. The TOE is compliant to the PSD PP and does not allow non-compliant devices.

Guidance Evaluator Assessment:

The Quick Installation Guides [19959], [19961], [19969] and [20601] have instructions to install the TOE.

Test Evaluator Assessment:

Test 1

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.

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	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 2

1. Check the TOE for radio frequency certification information to ensure that the TOE does not support wireless interfaces.

The evaluator has checked the TOE for radio frequency certification information and verified the TOE does not support wireless interfaces.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 3

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.

Steps 10 -13 not performed as the TOE does not support PS/2 interfaces.

The evaluator confirmed that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the Peripheral Device Connections (Appendix E)

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 1 - AO

1. Ensure the TOE is powered off. Ensure the TOE is powered off and connect an oscilloscope to the TOE audio input interface.
2. Connect an analog microphone to the TOE audio output peripheral interface.
3. Power on the TOE, speak loudly into the microphone from approximately one-inch distance, and verify no audio is present in the oscilloscope.
4. Disconnect the microphone and reconnect it to the TOE peripheral interface.
5. Speak loudly into the microphone from approximately one-inch distance, and verify no audio is present in the audio analyzer software.

The evaluator confirmed that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the Peripheral Device Connections.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 1 – KM

This test was repeated for each keyboard/mouse TOE peripheral interface. Steps 1-6 performed with the following unauthorized devices:

USB audio headset, USB camera, USB printer, USB authentication device connected to a TOE keyboard/mouse peripheral interface

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.
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.

The evaluator confirmed that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the Peripheral Device Connections.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 2 – KM

This test was repeated 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)

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.
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.

The evaluator confirmed that the TOE KM ports properly reject unauthorized devices and devices with unauthorized protocols as per the Peripheral Device Connections

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 1 – UA

This test was performed because condition “external” selected in FDP_PDC_EXT.4.1 is met.

This test was performed with an unauthorized device presenting itself as a composite device, a USB camera, a USB audio headset, a USB printer, a USB keyboard, a USB wireless dongle, and any device listed on the PSD UA blacklist.

1. Ensure the TOE is powered off and connected to a computer. Run USB analyzer software and open the real-time hardware console on the connected computer, and connect a USB sniffer to the unauthorized device.
2. Attempt to connect the unauthorized device via the USB sniffer to the TOE UA peripheral interface.
3. Power on the TOE. Verify the device is rejected.
4. Ensure the unauthorized device is disconnected from the TOE UA peripheral interface, then attempt to connect it again.
5. Verify the device is rejected.
6. Repeated steps 1-5 with a USB hub connected between the USB device and the USB sniffer and observed that the results are identical

The evaluator confirmed that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the Peripheral Device Connections.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 2 – UA

This test was performed because condition “external” selected in FDP_PDC_EXT.4.1 is met.

This test was performed with a USB device identified as User Authentication.

1. Ensure the TOE is powered off.
2. Connect the authorized device to the TOE peripheral interface.
3. Power on the TOE. Verify the TOE user indication described in the operational user guidance is not present.
4. Ensure the connected computer is selected and attempt to connect an authentication session. Verify that the authentication session.
5. Disconnect the authorized device, then reconnect it to the TOE peripheral interface.
6. Verify the TOE user indication described in the operational user guidance is not present.
7. Attempt to start an authentication session. Verify that the authentication session begins on the connected computer.

The evaluator confirmed that the TOE ports do not reject authorized devices with authorized protocols as per the Peripheral Device Connection Policy.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 1 – VI

This test was repeated for each of the selected protocols in FDP_PDC_EXT.3.1/VI: HDMI, DisplayPort

1. Connect the authorized device with an authorized protocol directly to a computer. Display any image on the device. Disconnect the device from the computer.
2. Configure the TOE and the Operational Environment in accordance with the operational guidance.
3. Ensure the TOE is powered off.
4. Connect the authorized device with an authorized protocol to the TOE peripheral interface.
5. Power on the TOE and verify the TOE user indication described in the operational user guidance is not present.
6. Ensure the connected computer is selected and verify that the device displays the same image as in step 1.
7. Disconnect the authorized device, then reconnect it to the TOE peripheral interface.
8. Verify the TOE user indication described in the operational user guidance is not present.
9. Verify that the device displays the same image as in step 1 and 6.

The evaluator confirmed that the TOE ports do not reject authorized devices and devices with authorized protocols as per the Peripheral Device Connections appendix in MOD_VI_V1.0.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

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

2.1.8.1 FDP_PDC_EXT.2.1/AO

The TSF shall allow connections with authorized devices as defined in [Appendix E] and [selection://n//n- authorized devices and functions as defined in the PP-Module for Keyboard/Mouse Devices,//n//n- authorized devices as defined in the PP-Module for User Authentication Devices,//n//n- authorized devices as defined in the PP-Module for Video/Display Devices,//n//n- no other device

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

2.1.8.2 FDP_PDC_EXT.2.2/AO

The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in [Appendix E] and [selection://n//n- authorized devices presenting authorized interface protocols as defined in the PP-Module for Keyboard/Mouse Devices,//n//n- authorized devices presenting authorized interface protocols as defined in the PP-Module for User Authentication Devices,//n//n- authorized devices presenting authorized interface protocols as defined in the PP-Module for Video/Display Devices,//n//n- no other devices

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

Application Note

The TSF must claim conformance to a PP-Configuration that includes each PP Module contained in any selections. The ST author should select all devices and interfaces supported by the TOE.

Evaluation Activity

Isolation Document

There are no Isolation Document EAs for this component.

TSS

There are no TSS EAs for this component.

Guidance

The evaluator shall verify that the operational guidance describes devices authorized for use with the TOE in accordance with the authorized peripheral device connections.

Test

The evaluator shall verify that the TOE 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 devices: analog headphone, and analog speakers.

Step 1: Ensure the TOE is powered off.

Step 2: Connect the authorized device to the TOE peripheral interface.

Step 3: Power on the TOE. Verify the TOE user indication described in the operational user guidance is not present.

Step 4: Play an audio file on the connected computer and verify the sound is heard through the authorized device.

Step 5: Disconnect the authorized device, then reconnect it to the TOE peripheral interface.

Step 6: Verify the TOE user indication described in the operational user guidance is not present.

Step 7: Play an audio file on the connected computer and verify the sound is heard through the authorized device.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

NA

Guidance Evaluator Assessment:

The quick install guides state which devices are authorized for use with the TOE.

Test Evaluator Assessment:

Test 1

1. Ensure the TOE is powered off.
2. Connect the authorized device to the TOE peripheral interface.
3. Power on the TOE. Verify the TOE user indication described in the operational user guidance is not present.
4. Play an audio file on the connected computer and verify the sound is heard through the authorized device.
5. Disconnect the authorized device, then reconnect it to the TOE peripheral interface.
6. Verify the TOE user indication described in the operational user guidance is not present.
7. Play an audio file on the connected computer and verify the sound is heard through the authorized device.

   The evaluator confirmed that the TOE ports do not reject authorized devices and devices with authorized protocols as per the authorized peripheral device connections.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

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

2.1.9.1 FDP_PDC_EXT.2.1/KM

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

- authorized devices as defined in the PP-Module for Audio Output Devices,

- authorized devices as defined in the PP-Module for User Authentication Devices,

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

- no other devices

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

2.1.9.2 FDP_PDC_EXT.2.2/KM

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

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

- authorized devices presenting authorized interface protocols as defined in the PP-Module for User Authentication Devices,

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

- no other devices

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

Application Note

The TSF must claim conformance to a PP-Configuration that includes each PP-Module contained in any selections. The ST author should select all devices and interfaces supported by the TOE.

If "authorized devices presenting authorized interface protocols as defined in the PP-Module for Video/Display Devices" is selected and "USB Type-C with DisplayPort as alternate function" is selected in FDP_PDC_EXT.3.1/Vid, then touch screen devices may not be used in conjunction with video devices that use USB Type-C with DisplayPort as alternate function.

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this SFR.

TSS

TSS evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.

Guidance

Guidance evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.

Test

Testing of this component is performed through evaluation of FDP_PDC_EXT.1 Test 2 as specified in [MOD_KM] section 2.1.7 above.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

NA

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

NA

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

2.1.10.1 FDP_PDC_EXT.3.1/KM

The TSF shall have interfaces for the [selection: USB (keyboard), USB (mouse)] protocols.

2.1.10.2 FDP_PDC_EXT.3.2/KM

The TSF shall apply the following rules to the supported protocols: [the TSF shall emulate any keyboard or mouse device functions from the TOE to the connected computer].

Application Note

It is expected that the ST author will make all selections in FDP_PDC_EXT.3.1/KM for which the TOE has an interface; the TOE boundary should encompass the entire device where possible.

If the TOE supports multiple connected computers (as specified by selecting "switching can be initiated only through express user action" in FDP_SWI_EXT.1.1 in the PSD PP), selections made in FDP_PDC_EXT.3.1 determine whether selection-based SFRs in Appendix B must be claimed. Specifically, selecting "USB (keyboard)" requires the TOE to claim FDP_RIP.1/KM and selecting both "USB (keyboard)" and "USB (mouse)" requires the TOE to claim FDP_SWI_EXT.3.

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this SFR.

TSS

The evaluator shall examine the TSS and verify it describes which types of peripheral devices that the PSD supports.

The evaluator shall examine the TSS to verify that keyboard or mouse device functions are emulated from the TOE to the connected computer.

Guidance

There are no guidance EAs for this component.

Test

Test activities for this SFR are covered under FDP_APC_EXT.1 tests 1-KM and 3-KM.

Evaluator Assessment

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

The TSS describes which peripherals are used in sections 9.1 to 9.5. Section 9.2.2.2 states that "…the keyboard and mouse function are emulated by the TOE".

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

NA

2.1.11 FDP_PDC_EXT.2/UA Authorized Devices (User Authentication Devices)

2.1.11.1 FDP_PDC_EXT.2.1/UA

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

- authorized devices as defined in the PP-Module for Audio Output Devices,

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

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

- no other devices

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

2.1.11.2 FDP_PDC_EXT.2.2/UA

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

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

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

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

- no other devices

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

Application Note

The TSF must claim conformance to a PP-Configuration that includes each PP-Module contained in any selections. The ST author should select all devices and interfaces supported by the TOE.

Evaluation Activity

The EAs for this SFR are performed as part of activities for FDP_PDC_EXT.1 above.

Evaluator Assessment

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

NA

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

NA

2.1.12 FDP_PDC_EXT.4 Supported Authentication Device

2.1.12.1 FDP_PDC_EXT.4.1

The TSF shall have an [selection: internal, external] user authentication device.

Application Note

The ST author must make the selection for the device which the TOE has: internal, external or both.

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this component.

TSS

The evaluator shall examine the TSS and verify that it describes whether the PSD has internal or external authentication devices.

Additional evaluation activities for STs that include the selection "external" are performed under FDP_PDC_EXT.1 in PSD PP.

Guidance

There are no guidance evaluation activities for this component.

Test

There are no test evaluation activities for this component.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.2.4 of the TSS describes the authentication devices. They are Smart Card readers and thus are external devices.

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

NA

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

2.1.13.1 FDP_PDC_EXT.2.1/VI

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

- authorized devices as defined in the PP-Module for Audio Output Devices,

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

- authorized devices as defined in the PP-Module for User Authentication Devices,

- no other devices

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

2.1.13.2 FDP_PDC_EXT.2.2/VI

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

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

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

- authorized devices presenting authorized interface protocols as defined in the PP-Module for User Authentication Devices,

- no other devices

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

Application Note

The TSF must claim conformance to a PP-Configuration that includes each PP-Module contained in any selections. The ST author should select all devices and interfaces supported by the TOE.

If "authorized devices presenting authorized interface protocols as defined in the PP-Module for Keyboard/Mouse" is selected and "USB Type-C with DisplayPort as alternate function" is selected in FDP_PDC_EXT.3.1/VI, then video devices that use USB Type-C with DisplayPort as alternate function may not be used in conjunction with touch screen devices.

Evaluation Activity

Isolation Document

There are no Isolation Document EAs for this component.

TSS

TSS evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.

Guidance

Guidance evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.

Test

Testing of this component is performed through evaluation of FDP_PDC_EXT.1 as specified in section 2.1.7 above.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

NA

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

NA

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

2.1.14.1 FDP_PDC_EXT.3.1/VI

The TSF shall have interfaces for the [selection: VGA, DVI-D, DVI-I, HDMI, DisplayPort, USB Type-C with DisplayPort as alternate function] protocols.

2.1.14.2 FDP_PDC_EXT.3.2/VI

The TSF shall apply the following rules to the supported protocols: [the TSF shall read the connected display EDID information once during power-on or reboot [selection: automatically, when prompted by user intervention]]. ***Note: TD0620 applied***

Application Note

It is expected that the ST author will make all selections in FDP_PDC_EXT.3.1/VI for which the TOE has an interface; the TOE boundary should encompass the entire device where possible.

If the KM PP-Module is also claimed by the ST, "USB Type-C with DisplayPort as alternate function" may not be selected in conjunction with a touchscreen peripheral device.

If "DisplayPort" is selected, the ST must include the selection-based requirement FDP_IPC_EXT.1.

This PP-Module defines several iterations of FDP_SPR_EXT.1. Depending on the selections made in FDP_PDC_EXT.3.1/VI, the evaluator must include the relevant iterations.

If the TOE can read the connected display EDID information during power-on or reboot without human intervention, the first selection item for FDP_PDC_EXT.3.2/VI is selected. If the TOE requires human intervention to read the connected display EDID during power-on or reboot, the second selection item is selected. ***Note: TD0620 applied***

Evaluation Activity

Isolation Document

There are no Isolation Document EAs for this component.

TSS

TSS evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.

Guidance

Guidance evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.

Test

Testing of this component is performed through evaluation of FDP_APC_EXT.1 as specified in section 2.1.5 above.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

NA

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

NA

2.1.15 FDP_PUD_EXT.1 Powering Unauthorized Devices

2.1.15.1 FDP_PUD_EXT.1.1

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

Evaluation Activity

Isolation Document

There are no Isolation Document EAs for this component.

TSS

The evaluator shall verify the TSS states that the TOE does not supply power to an unauthorized device connected to the analog audio output interface.

The evaluator shall also verify that the TOE cannot be configured to supply power to a device connected to the analog audio output interface.

Guidance

The evaluator shall verify that the guidance states that a microphone should never be connected to the TOE's analog audio output interface.

Test

Step 1: Connect the amplified speakers directly to computer #1's analog audio output interface (typically green in color). Set the volume at the speakers to approximately 25%.

Step 2: Connect the computer interface audio cable to the TOE audio output computer interface and computer #1's analog audio microphone input interface (typically pink in color) instead of the computer analog audio output interface.

Evaluator note: There is no step 3 in [MOD_AO_SD].

Step 4: Connect an open 3.5 millimeter stereo plug to the TOE analog audio peripheral interface.

Step 5: Power up the TOE and ensure computer #1 is selected.

Step 6: Measure the DC voltage of stereo plug from the TOE analog audio peripheral interface between the ground terminal and each one of the other two terminals (tip and ring) using a digital voltmeter.

Step 7: Verify the voltage is 0.2 volts or less, ensuring there is no DC bias voltage supplied to the microphone.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.2.5 of the TSS states "The TOE does not supply power to the analog audio output interface and cannot be configured to do so. Therefore, it cannot be used to supply power to an unauthorized device on that interface."

Guidance Evaluator Assessment:

The [CC_Supp] states in section 1.1 "Microphones must not be plugged into the TOE audio output interfaces."

Test Evaluator Assessment:

Test 1

1. Connect the amplified speakers directly to computer #1's analog audio output interface (typically green in color). Set the volume at the speakers to approximately 25%.

2. Connect the computer interface audio cable to the TOE audio output computer interface and computer #1's analog audio microphone input interface (typically pink in color) instead of the computer analog audio output interface.
3. Connect an open 3.5-millimetre stereo plug to the TOE analog audio peripheral interface.
4. Power up the TOE and ensure computer #1 is selected.
5. Measure the DC voltage of stereo plug from the TOE analog audio peripheral interface between the ground terminal and each one of the other two terminals (tip and ring) using a digital voltmeter.
6. Verify the voltage is 0.2 volts or less, ensuring there is no DC bias voltage supplied to the microphone.

The evaluator confirmed that the TSS states that the TOE does not supply power to an unauthorized device connected to the analog audio output interface.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

2.1.16 FDP_PWR_EXT.1 Powered By Computer

2.1.16.1 FDP_PWR_EXT.1.1

The TSF shall not be powered by a connected computer.

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this component.

TSS

The evaluator shall examine the TSS and verify that the connected computer does not power the TOE.

Guidance

There are no guidance EAs for this component.

Test

The evaluator shall perform the following test for each connected computer:

Step 1: Ensure the power source is disconnected from the TOE.

Step 2: Connect a USB sniffer between a TOE UA computer interface and its computer, attempt to turn on the TOE, and verify the TOE is not powered on, the user authentication device is not present in the real time hardware console, and no traffic is captured in the USB sniffer.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.2.4 of the TSS states that "The user authentication device must be able to receive power from the TOE. An external power source, such as power from the connected computer, is prohibited for this interface."

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

Test 1

1. Ensure the power source is disconnected from the TOE.
2. Connect a USB sniffer between a TOE UA computer interface and its computer, attempt to turn on the TOE, and verify the TOE is not powered on, the user authentication device is not present in the real time hardware console, and no traffic is captured in the USB sniffer.

The evaluator confirmed they performed the above test for each connected computer. No user authentication device is present, and no traffic was captured in the USB sniffer.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

2.1.17 FDP_SWI_EXT.1 PSD Switching

2.1.17.1 FDP_SWI_EXT.1.1

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

Application Note

If "switching can be initiated only through express user action" is selected, the ST must include the selection-based requirements FDP_SWI_EXT.2 and FTA_CIN_EXT.1.

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this component.

TSS

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.

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.

Guidance

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.

Test

There are no test Evaluation Activities for this component.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.2.1 states that "The user determines the host computer to be connected to the peripherals by pressing a button on the TOE front panel, or on the Auxiliary Front Panel (AFP). Switching can only be initiated through express user action.

Matrix and combiner devices may be switched with peripheral devices using a guard. This is done by moving the mouse to the edge of the screen while pressing the left CTRL key."

Guidance Evaluator Assessment:

The [19959], [19961], [19969] and the [20601] explain the device switching mechanisms. The [ADMIN] also has a "Warnings and Precautions" section which explains the limitations of the TOE.

Test Evaluator Assessment:

NA

2.1.18 FDP_RIP_EXT.1 Residual Information Protection

2.1.18.1 FDP_RIP_EXT.1.1

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

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this component.

TSS

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.

The evaluator shall verify that the Letter of Volatility provides assurance that user data is not stored in TOE non-volatile memory or storage.

Guidance

There are no guidance Evaluation Activities for this component.

Test

There are no test Evaluation Activities for this component.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

The Letter of Volatility is provided as an annex, Annex A of the [ST]. It lists each component and explains which have volatile or non-volatile memory. It also states whether data is retained or not. The power source for each component is listed.

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

NA

2.1.19 FDP_TER_EXT.1 Session Termination

2.1.19.1 FDP_TER_EXT.1.1

The TSF shall terminate an open session upon removal of the authentication element.

Evaluation Activity

Isolation Document

There are no Isolation Document activities for this component.

TSS

The evaluator shall examine the TSS and verify that the TOE terminates an open session upon removal of the authentication element.

Guidance

The evaluator shall examine the guidance documentation and verify that the TOE terminates an open session upon removal of the authentication element.

Test

Testing for this component is performed as part of FDP_APC_EXT.1 test 2-UA.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.2.4 states “Removal of the authentication device will also close the authentication session.” Once the authentication device is removed, the session is terminated.

Guidance Evaluator Assessment:

Section 4.6 of the [CC_Supp] states “An open authentication device session is terminated on removal of the smartcard, authentication device, or when the device is switched to a different computer.”

Test Evaluator Assessment:

NA

2.1.20 FDP_UAI_EXT.1 User Authentication Isolation

2.1.20.1 FDP_UAI_EXT.1.1

The TSF shall isolate the user authentication function from all other TOE USB functions.

Application Note

This SFR requires additional information for the Isolation Documentation and Assessment. Refer to Appendix D for this information.

Evaluation Activity

Isolation Document

The evaluator shall examine the Isolation Documentation and verify that it describes how the TOE enforces user authentication *isolation from other TOE USB functions.*

TSS

The evaluator shall examine the TSS and verify that it states that the TOE has separate USB connections for user authentication functions and any other USB functions.

Guidance

The evaluator shall examine the guidance and verify that it states that the TOE has separate USB connections for user authentication functions and any other USB functions.

Test

Test 1

This test verifies that UA functionality is not sent to other USB interfaces.

Perform this test for each computer interface.

Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect a display directly to each connected computer. Run USB protocol analyzer software and open a real-time hardware information console and a text editor on each connected computer. Ensure an authorized user authentication device is connected.

Perform steps 2-4 for each TOE USB peripheral interface other than UA.

Step 2: Connect a USB sniffer to the TOE USB peripheral interface.

Step 3: Connect an authentication session and verify no traffic is captured on the USB sniffer.

Step 4: Disconnect the USB sniffer and the authentication session.

Perform steps 5-7 for each TOE USB computer interface other than UA.

Step 5: Connect a USB sniffer to the TOE USB computer interface and ensure that computer is selected.

Step 6: Connect an authentication session and verify no traffic is captured on the USB sniffer.

Step 7: Disconnect the USB sniffer and the authentication session.

Step 8: Power down the TOE.

Step 9: For each TOE USB interface (peripheral device and computer) other than UA, connect the USB sniffer and verify no traffic is captured.

Test 2

[Conditional: Perform this test only if the TOE supports KM functionality.]

This test verifies that KM functionality is not sent to UA interfaces.

Perform this test while the TOE is powered on and powered off.

Step 1: Connect a KM device to the TOE KM peripheral interface.

Perform steps 2-3 for each TOE UA computer interface.

Step 2: Connect a USB sniffer to the TOE UA computer interface.

Step 3: Exercise the functions of the peripheral device type(s) selected in FDP_PDC_EXT.3.1/KM in MOD_KM_V1.0 and verify that no traffic is sent and captured on the USB sniffer.

[Conditional: Perform steps 4-5 only if "external" is selected in FDP_PDC_EXT.4.1]

Step 4: Disconnect the USB sniffer and connect it to the TOE UA peripheral device interface.

Step 5: Exercise the functions of the peripheral device type(s) selected in FDP_PDC_EXT.3.1/KM in MOD_KM_V1.0 and verify that no traffic is sent and captured on the USB sniffer.

Test 3

[Conditional: Perform this test only if the TOE supports video functionality and "USB Type-C with DisplayPort as alternate function" is selected in FDP_PDC_EXT.3.1/VI in MOD_VI_V1.0.]

This test verifies that USB video functionality is not sent to UA interfaces.

Perform this test while the TOE is powered on and powered off.

Perform steps 1-3 for each TOE UA computer interface and TOE USB type-C video peripheral interface.

Step 1: Connect a USB sniffer to the TOE UA computer interface.

Step 2: Connect a monitor to the TOE USB type-C video peripheral interface and verify that no traffic is sent and captured on the USB sniffer.

Step 3: Play a video on the selected computer and verify that no traffic is sent and captured on the USB sniffer.

[Conditional: Perform steps 4-7 only if "external" is selected in FDP_PDC_EXT.4.1]

Step 4: Disconnect the monitor.

Step 5: Disconnect the USB sniffer and connect it to the TOE UA peripheral device interface.

Step 6: Reconnect the monitor to the TOE USB type-C video peripheral interface and verify that no traffic is sent and captured on the USB sniffer.

Step 7: Play a video on the selected computer and verify that no traffic is sent and captured on the USB sniffer.

Isolation Document Evaluator Assessment:

In the [Isol] doc, figure 10 indicates the authentication device isolation. Section 3.8.1 describes the KVM device isolation.

TSS Evaluator Assessment:

Section 9.2.4 of the TSS says that authentication device functions are separate and physically isolated from the keyboard and mouse functions.

Guidance Evaluator Assessment:

The Quick Install Guides and [Isol] section2.3 state the type of USB devices that may be used. Authentication devices have separate connections than other devices.

Test Evaluator Assessment:

Test 1

1. Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect a display directly to each connected computer. Run USB protocol analyzer software and open a real-time hardware information console and a text editor on each connected computer. Ensure an authorized user authentication device is connected.
2. Connect a USB sniffer to the TOE USB peripheral interface.
3. Connect an authentication session and verify no traffic is captured on the USB sniffer.
4. Disconnect the USB sniffer and the authentication session.
5. Connect a USB sniffer to the TOE USB computer interface and ensure that computer is selected.
6. Connect an authentication session and verify no traffic is captured on the USB sniffer.
7. Disconnect the USB sniffer and the authentication session.
8. Power down the TOE.
9. For each TOE USB interface (peripheral device and computer) other than UA, connect the USB sniffer and verify no traffic is captured.

The evaluator confirmed that user authentication functionality is not sent to other USB interfaces.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 2

1. Connect a KM device to the TOE KM peripheral interface.
2. Connect a USB sniffer to the TOE UA computer interface.
3. Exercise the functions of the peripheral device type(s) selected in FDP_PDC_EXT.3.1/KM in MOD_KM_V1.0 and verify that no traffic is sent and captured on the USB sniffer.
4. Disconnect the USB sniffer and connect it to the TOE UA peripheral device interface.
5. Exercise the functions of the peripheral device type(s) selected in FDP_PDC_EXT.3.1/KM in MOD_KM_V1.0 and verify that no traffic is sent and captured on the USB sniffer.

The evaluator confirmed that KM functionality is not sent to UA interfaces.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 3

NA

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

2.1.21.1 FDP_UDF_EXT.1.1/AO

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

Application Note

For audio signals, the TOE analog audio output computer interface is considered to be unidirectional if it receives no signal greater than 45 dB of attenuation at the extended audio frequency range. It is very unlikely that this element can be satisfied unless all unselected computer interfaces are shorted to ground by the TSF.

If the peripheral interface supports multiple signals (such as right and left audio, or audio bias), then all those supported signals should comply with the above SFR.

Evaluation Activity

Isolation Document

The evaluator shall examine the Isolation Documentation to determine that it describes how the TOE enforces audio output data flow isolation from other TOE functions, such that the audio output peripheral interface is unidirectional and no data can be routed from a connected peripheral back to a connected computer. The description shall ensure the signal attenuation between any TOE audio output peripheral device interface and any other TOE computer audio output interface is at least 45 dB measured with a 2V input pure sine wave at the extended audio frequency range, including negative swing signal.

TSS

There are no TSS EAs for this component.

Guidance

There are no guidance EAs for this component.

Test

Note: Data is considered not to transit the TOE if no signal greater than 45 dB of attenuation at the specific audio frequency is received.

The evaluator shall perform the following test:

Step 1: Connect a computer to the TOE analog audio output peripheral interface, run its tone generator software, and run audio analyzer software on the connected computer.

Step 2: Perform steps 3-6 for each TOE analog audio output peripheral interface.

Step 3: For each connected computer, ensure it is selected, use the tone generator on the computer connected to the TOE analog audio output peripheral interface to generate the designated frequencies, and verify that the audio is not present on the selected computer's audio analyzer software.

Step 4: Replace the selected computer with an oscilloscope and connect an external audio signal generator to the TOE analog audio output peripheral interface. Perform step 5 with the signal generator set to the following settings:

- Pure sine wave around the average voltage of half output (positive signal only), with the output signal set to 2.00 V peak-to-peak, calibrating the signal with the oscilloscope as needed;

- Signal average to 0V (negative swing)

Step 5: Set the signal generator to generate the designated frequencies, and verify the signal on the oscilloscope is 11.2 mV or less.

Isolation Document Evaluator Assessment:

Section 3.5.3 of the [Isol] document states "Isolated interfaces and components are used, as are audio data diodes. There are no shared parts." It then goes on to explain the isolation. Section 3.5.4 describes how the audio output is isolated from the USB paths.

TSS Evaluator Assessment:

NA

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

Test 1

1. Connect a computer to the TOE analog audio output peripheral interface, run its tone generator software, and run audio analyzer software on the connected computer.
2. Perform steps 3-6 for each TOE analog audio output peripheral interface.
3. For each connected computer, ensure it is selected, use the tone generator on the computer connected to the TOE analog audio output peripheral interface to generate the designated frequencies, and verify that the audio is not present on the selected computer's audio analyzer software.
4. Replace the selected computer with an oscilloscope and connect an external audio signal generator to the TOE analog audio output peripheral interface. Perform step 5 with the signal generator set to the following settings:
   - Pure sine wave around the average voltage of half output (positive signal only), with the output signal set to 2.00 V peak-to-peak, calibrating the signal with the oscilloscope as needed;
   - Signal average to 0V (negative swing)

5. Set the signal generator to generate the designated frequencies and verify the signal on the oscilloscope is 11.2 mV or less.

The evaluator confirmed the TOE audio output peripheral interface is unidirectional and no data can be routed from a connected peripheral back to a connected computer.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

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

2.1.22.1 FDP_UDF_EXT.1.1/KM

The TSF shall ensure [selection: keyboard, mouse] data transits the TOE unidirectionally from the [TOE [selection: keyboard, mouse]] peripheral interface(s) to the [TOE [selection: keyboard, mouse]] interface.

Application Note

Caps Lock, Num Lock, and Scroll Lock indications may be displayed by the TOE while still not passing that information to the keyboard.

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this SFR.

TSS

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.

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.

Guidance

There are no guidance EAs for this component.

Test

Test activities for this SFR are covered under FDP_APC_EXT.1 test 3-KM.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.2.2.1 of the TSS explains how the flows to the keyboard/mouse are unidirectional. “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.”

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

NA

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

2.1.23.1 FDP_UDF_EXT.1.1/VI

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

Evaluation Activity

Isolation Document

There are no Isolation Document EAs for this component.

TSS

There are no TSS EAs for this component.

Guidance

There are no guidance EAs for this component.

Test

This component is evaluated through evaluation of FDP_APC_EXT.1 as specified in section 2.1.5 above.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

NA

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

NA

2.1.24 FDP_AFL_EXT.1 Audio Filtration

2.1.24.1 FDP_AFL_EXT.1.1

The TSF shall ensure outgoing audio signals are filtered as per [Audio Filtration Specifications table]. (Please refer to mod_ao_v1.0.pdf page 13 for the table.)

Application Note

The above security requirement is designed to reduce the likelihood that speakers emitting a signaling event at frequencies outside the range of human hearing could be successfully used to bridge an air-gap to another computer.

Evaluation Activity

Isolation Document

There are no Isolation Document EAs for this component.

TSS

The evaluator shall check the TSS to verify that the TOE audio function implementation properly filters the audio passing through the TOE.

Guidance

There are no guidance EAs for this component.

Test

Step 1: Connect a computer to the TOE analog audio output peripheral interface and run audio analyzer software on it.

Step 2: For each connected computer, ensure it is selected, use its tone generator software to generate a sine wave audio tone for each of the frequencies in the Audio Filtration Specifications table and verify in the audio analyzer software that they are attenuated by at least the amount specified in the Audio Filtration Specifications table.

Step 3: Connect an oscilloscope to the TOE analog audio output peripheral interface and set it to measure the peak-to-peak voltage.

Step 4: For each connected computer, perform step 5 with the signal generator set to the following settings:

- Pure sine wave around the average voltage of half output (positive signal only), with the output signal set to 2.00 V peak-to-peak, calibrating the signal with the oscilloscope as needed

- Signal average to 0V (negative swing)

Step 5: Set the signal generator to generate the frequencies in Audio Filtration Specifications table and verify the signal on the oscilloscope does not exceed the corresponding maximum voltage after attenuation.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.2.5 of the TSS states “Unidirectional flow data diodes prevent audio data flow from an audio device to a selected computer. There is a separate audio interface for each computer. Each interface is electrically isolated from other interfaces, and from other TOE circuitry. These features ensure that the audio filtration specification requirements are met.

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

1. Connect a computer to the TOE analog audio output peripheral interface and run audio analyzer software on it.
2. For each connected computer, ensure it is selected, use its tone generator software to generate a sine wave audio tone for each of the frequencies in the Audio Filtration Specifications table and verify in the audio analyzer software that they are attenuated by at least the amount specified in the Audio Filtration Specifications table.
3. Connect an oscilloscope to the TOE analog audio output peripheral interface and set it to measure the peak-to-peak voltage.
4. For each connected computer, perform step 5 with the signal generator set to the following settings:
   • Pure sine wave around the average voltage of half output (positive signal only), with the output signal set to 2.00 V peak-to-peak, calibrating the signal with the oscilloscope as needed.
   • Signal average to 0V (negative swing).
5. Set the signal generator to generate the frequencies in Audio Filtration Specifications table and verify the signal on the oscilloscope does not exceed the corresponding maximum voltage after attenuation.

The evaluator confirmed that the TOE audio function implementation properly filters the audio passing through the TOE.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

2.2 Protection of the TSF (FPT)

2.2.1 FPT_FLS_EXT.1 Failure with Preservation of Secure State

2.2.1.1 FPT_FLS_EXT.1.1

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

Application Note

In the context of this PP, a 'secure state' is defined by the TOE disabling all peripheral and connected computer interfaces when the correctness of its own functions cannot be assured.

Failure of the anti-tamper function should be selected if FPT_PHP.3 is included in the ST.

Evaluation Activity

This SFR is evaluated in conjunction with FPT_TST.1.

Evaluator Assessment:

NA Tested with FPT_TST.1

2.2.2 FPT_NTA_EXT.1 No Access to TOE

2.2.2.1 FPT_NTA_EXT.1.1

TOE firmware, software, and memory shall not be accessible via the TOE's external ports, with the following exceptions: [selection: the Extended Display Identification Data (EDID) memory of Video TOEs may be accessible from connected computers; the configuration data, settings, and logging data that may be accessible by authorized administrators; no other exceptions].

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this component.

TSS

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.

Guidance

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

Test

There are no test Evaluation Activities for this component.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.4.1 of the TSS says that an administrator may use a connected computer to access EDID memory, configuration data and audit data. The TOE microcontrollers run from inside protected flash memory. The firmware cannot be accessed or read by JTAG tools. The FW executes in SRAM and has tamper protections.

Guidance Evaluator Assessment:

The [ADMIN] states "The product enables authorized administrators to download event log files and audit the product history as well as have access to advanced settings. This function is available only to authenticated administrators. "

The Quick Install Guides [19959], [19961], [19969] and [20601] have a warning that there is active tamper detection in the device or that tamper evident seals are being used on the device.

Test Evaluator Assessment:

NA

2.2.3 FPT_PHP.1 Passive Detection of Physical Attack

2.2.3.1 FPT_PHP_1.1

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

2.2.3.2 FPT_PHP_1.2

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

Application Note

FPT_PHP.1.1 include indications generated from application of optional SFR FPT_PHP.3

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this component.

TSS

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.

Guidance

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.

Test

Test 1: The evaluator shall verify, for each tamper evident seal or label affixed to the TOE enclosure 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 2: The evaluator shall verify that it is not possible to administratively disable or otherwise prevent the display of any tampering indicators.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.4.2.1. and 9.4.2.2 explain the anti-tamper mechanisms. The tamper evident seals are described in section 9.4.2.1. If a seal is removed, the word VOID appears to indicate the TOE has been tampered.

In section 9.4.2.2 The TSS discusses the active tamper mechanisms. Once a device is tampered, it is inoperable. Tampering causes a small fuse to melt and renders the device inoperable.

Guidance Evaluator Assessment:

The Quick Installation Guides [19959], [19961], [19969] and [20601' have a note on tamper. "Anti-Tampering System: This HSL high security product is equipped with an always-on active anti-tampering system. If mechanical intrusion is detected, the product is permanently disabled and abnormal LED behavior is activated, with all LEDs blinking continuously."

The [ADMIN] states "The product is equipped with always-on active anti- tampering system. Any attempt to open the product activates the anti-tamper triggers and renders the unit inoperable and the warranty void."

Test Evaluator Assessment:

Test 1

1. Removed the tamper evident seals from the TOE.

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.

Units Tested	**DK82PH-4**
Result	PASS

Test 2

1. Attempt to remove the tamper evident seals from the TOE without damaging the tampering indicators.

The evaluator confirmed that it is not possible to administratively disable or otherwise prevent the display of any tampering indicators.

Units Tested	**DK82PH-4**
Result	PASS

2.2.4 FPT_TST.1 TSF Testing

2.2.4.1 FPT_TST.1.1

The TSF shall run a suite of self-tests [during initial start-up and at the conditions [selection: upon reset button activation, no other conditions]] to demonstrate the correct operation of [user control functions and [selection: active anti-tamper functionality, no other functions]].

2.2.4.2 FPT_TST.1.2

The TSF shall provide authorized users with the capability to verify the integrity of [selection: [assignment: parts of TSF data], TSF data].

2.2.4.3 FPT_TST.1.3

The TSF shall provide authorized users with the capability to verify the integrity of [selection: [assignment: parts of TSF], TSF].

Application Note

Reset button activation should be selected if the TOE includes such functionality.

If "active anti-tamper functionality" is selected, portions of the evaluation activities will test functions from the optional active anti-tamper SFR FPT_PHP.3.

Anyone with physical access to the TOE can be considered an authorized user.

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this component.

TSS

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).

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.

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.

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.

Guidance

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.

Test

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 the operational guidance.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.4.4 of the TSS discusses the self-test and what it encompasses:

- Verification of the front panel push-buttons
- Verification of the integrity of the microcontroller firmware

- Verification of computer port isolation. This is tested by sending test packets to various interfaces and attempting to detect this traffic at all other interfaces

If the self-test fails, the front panel LEDs blink and the TOE makes a clicking sound. The TOE can be rebooted to clear the error and the self-test is rerun. All errors are logged.

Guidance Evaluator Assessment:

The quick installation Guides [19959], [19961], [19969], and [20601] state “As the product powers-up it performs a self-test procedure. In case of self- test failure for any reason, including jammed buttons, the product will be Inoperable and self-test failure will be indicated by abnormal LED behavior.”

The [ADMIN] states “As the product powers-up it performs a self-test procedure. In case of a self-test failure, including jammed buttons, the product will be Inoperable. A Self-test failure is indicated by the following abnormal LED behavior:

- All channel-select LEDs are turned ON and then OFF;
- A specific, predefined LED combination is turned ON;
- The predefined LED combination indicates the problem type (jammed buttons, firmware integrity)

Section 4.2 of the [CC_Supp] describes the self-test and failure behaviour and advises to contact HSL technical support if rebooting does not clear the failure.

Test Evaluator Assessment:

1. The TOE must be powered off, ensure the power cable is removed from the TOE before proceeding.
2. Firmly press and hold channel 1 button 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 video/keyboard/mouse is being output from the TOE while it is in self-test failure state.

The evaluator confirmed that that successful completion of the self-tests can be determined by following the corresponding steps in operational guidance.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

2.2.5 FPT_TST_EXT.1 TSF Testing

2.2.5.1 FPT_TST_EXT.1.1

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

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this component.

TSS

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.

Guidance

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.

The evaluator shall verify that the operational user guidance provides adequate information on TOE self-test failures, their causes, and their indications.

Test

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.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

The TSS section 9.4.4 states that the TOE front panel LEDs blink when a self-test fails. The TOE disables the switching functionality and remains in a disabled state until the self-test is rerun and passes. Self-test failures are recorded in the log file with the date and time.

Guidance Evaluator Assessment:

The quick installation Guides [19959], [19961], [19969] and [20601] state "As the product powers-up it performs a self-test procedure. In case of self- test failure for any reason, including jammed buttons, the product will be Inoperable and self-test failure will be indicated by abnormal LED behavior."

The [ADMIN] states "As the product powers-up it performs a self-test procedure. In case of a self-test failure, including jammed buttons, the product will be Inoperable. A Self-test failure is indicated by the following abnormal LED behavior:

- All channel-select LEDs are turned ON and then OFF;
- A specific, predefined LED combination is turned ON;
- The predefined LED combination indicates the problem type (jammed buttons, firmware integrity)

Section 4.2 of the [CC_Supp] describes the self-test and failure behavior and advises to contact HSL technical support if rebooting does not clear the failure.

Test Evaluator Assessment:

Test 1

1. The TOE must be powered off, ensure the power cable is removed from the TOE before proceeding.
2. Firmly press and hold channel 1 button 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 video/keyboard/mouse is being output from the TOE while it is in self-test failure state.

The evaluator confirmed that the TOE does perform a self-test failure and that the TOE responds by disabling normal functions and provides proper indications to the user.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

3 Evaluation Activities for Optional Requirements

3.1 User Data Protection (FDP)

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

3.1.1.1 FDP_FIL_EXT.1.1/KM

The TSF shall have [selection: configurable, fixed] device filtering for [selection: keyboard, mouse] interfaces.

3.1.1.2 FDP_FIL_EXT.1.2/KM

The TSF shall consider all [PSD KM] blacklisted devices as unauthorized devices for [selection: keyboard, mouse] interfaces in peripheral device connections.

3.1.1.3 FDP_FIL_EXT.1.3/KM

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

Application Note

The ST author must make the selections for the device which the TOE has: configurable or fixed or both; and keyboard or mouse or both.

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this SFR.

TSS

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.

Guidance

[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.

Test

Test 1

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 2

[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.

Step 1: Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance.

Step 2: Connect to the TOE KM peripheral device interface a composite device which contains a HID class and a non-HID class.

Step 3: Configure the TOE KM CDF to whitelist the composite device.

Step 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.

Step 5: Configure the TOE KM CDF to blacklist the device.

Step 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.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

NA - The selection is fixed – blacklisted devices are unauthorized and whitelisted devices are authorized.

Guidance Evaluator Assessment:

NA – the configuration is fixed.

Test Evaluator Assessment:

Test 1

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.

All devices on the PSD KM blacklist were tested and are rejected as expected. The evaluator confirmed that the blacklist in place rejects all devices found in step 2.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

Test 2

NA “Configurable” has not been selected. Therefore, this evaluation activity is not applicable.

3.1.2 FDP_RDR_EXT.1 Re-Enumeration Device Rejection

3.1.2.1 FDP_RDR_EXT.1.1

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

Application Note

This SFR should prevent devices that change their class from authorized to unauthorized, but cannot prevent malicious devices that use an authorized HID-class.

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this SFR.

TSS

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.

Guidance

There are no guidance EAs for this component.

Test

The evaluator shall use a BadUSB, programmable keyboard, and/or USB Rubber Ducky as a malicious USB device to perform the following test:

Step 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 the real-time hardware information console.

Step 2: Configure the malicious USB device as a HID-class device and to re-enumerate as a mass storage device.

Step 3: Connect the malicious USB device to the TOE KM peripheral interface.

Step 4: Power on the TOE and activate the re-enumeration after 1 minute.

Step 5: 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.

Step 6: Remove the malicious USB device and reconfigure as a HID-class device and to re-enumerate as a mass storage device.

Step 7: Connect the malicious USB device to the TOE KM peripheral interface and activate the reenumeration after 1 minute.

Step 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.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.2.2.1 discusses Keyboard and Mouse Enumeration. 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.

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.

Section 9.2.2.4 states "If a connected device attempts to re-enumerate as a different USB device type, it will be rejected by the TOE."

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

Test 1

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.

The evaluator configured the USB device accordingly to verify device rejection and ensured the TOE properly enforced security protocols.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

3.1.3 FDP_RIP_EXT.2 Purge of Residual Information

3.1.3.1 FDP_RIP_EXT.2.1

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

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this component.

TSS

The evaluator shall verify that the TSS describes the TOE's reaction to memory purge or restore factory defaults.

The evaluator shall verify that the Letter of Volatility included in the TSS describes the effect that the TOE Restore Factory Default function has on each component listed in the Letter of Volatility.

Guidance

The evaluator shall check that the operational user guidance provides a method to purge TOE memory or to restore factory default settings.

Test

Step 1: Perform the TOE memory purge or restore factory defaults according to the guidance and verify that the TOE enters a desirable secure state.

The evaluator shall check that the log record is not deleted if a logging function is supported by the TOE.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.2.1.3 of the TSS discusses what occurs if a factory reset occurs. The username and password of the primary administrator are not reset and critical logs are not reset. The letter of volatility is also appended to the ST in Annex A.

Guidance Evaluator Assessment:

[ADMIN] states "The log data may not be erased and log functions may not be disabled by users or administrators. RFD does not reset the administrator's password and username but deletes the additional users that the admin has created."

Also, "Product power-up and RFD behavior:
a. By default, after product power-up, the active channel will be computer #1, indicated by the lit applicable front panel push button LED.
b. To reset the device to factory defaults, please use: Left CTRL | Left CTRL | f11 | r.
c. RFD action is indicated by all the front panel LEDs blinking together
d. When the product boots after RFD, the keyboard and mouse are mapped to the active channel #1 and default settings are restored, erasing all user-set definitions."

Test Evaluator Assessment:

Test 1

The test case for this SFR is covered by FAU_GEN.1 Steps 7-9.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

3.2 Protection of the TSF (FPT)

3.2.1 FPT_PHP.3 Resistance to Physical Attack

3.2.1.1 FPT_PHP.3.1

The TSF shall resist [a physical attack for the purpose of gaining access to the internal components, to damage the anti-tamper battery, to drain or exhaust the anti-tamper battery] to the [TOE enclosure] by becoming permanently disabled.

Application Note

'Becoming permanently disabled' is interpreted to mean that connected peripheral devices will cease to function.

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this component.

TSS

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.

Guidance

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.

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.

Test

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.

Note that it is obvious that if the TOE was physically tampered with, then the attacker may easily circumvent the tamper indication means (for example cut the relevant TOE front panel wires). Nevertheless, the following test verifies that the user would be unable to ignore the TOE tampering indications and resume normal work.

The evaluator shall perform the following steps:

Step 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 indication that it has been tampered with in accordance with the operational user guidance.

Step 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. ***Note: TD0583 applied***

Step 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.

Step 4: The evaluator shall acquire a copy of the TOE that has been previously tampered with.

Step 5: The evaluator shall power on the TOE and verify that the tampering indicator is displayed.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.4.2.2 of the TSS 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. Any attempt to separate the pieces of the enclosure to access the internal circuitry will trigger the anti-tampering function. Power is provided to the circuitry by the TOE power supply and by a backup battery. If the self-test detects that the battery is depleted or failing, the anti-tampering function will be triggered.

Guidance Evaluator Assessment:

The Quick Installation Guides [19959], [19961], [19969] and [20601] have a note on tamper. "Anti-Tampering System: This HSL high security product is equipped with an always-on active anti-tampering system. If mechanical intrusion is detected, the product is permanently disabled and abnormal LED behavior is activated, with all LEDs blinking continuously."

The [ADMIN] states "The product is equipped with always-on active anti- tampering system. Any attempt to open the product activates the anti-tamper triggers and renders the unit inoperable and the warranty void."

Test Evaluator Assessment:

Test 1

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. Note: TD0583 applied
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.

The evaluator confirmed that the test execution steps were performed on all the units detailed in the units tested section. The same execution output was observed for each model tested.

Units Tested	**DK82PH-4**
Result	PASS

4 Selection-Based Requirements

4.1 Security Audit (FAU)

4.1.1 FAU_GEN.1 Audit Data Generation

Note: This SFR is optional in the base PP. Inclusion of [MOD_UA] re-categorized it as selection-based. It shall be included in the TSF if ‘configurable’ is selected in FDP_FIL_EXT.1.1/UA.

Note: This SFR is optional in the base PP. Inclusion of [MOD_KM_V1.0] re-categorized it as selection-based. It shall be included in the TSF if ‘configurable’ is selected in FDP_FIL_EXT.1.1/KM.

4.1.1.1 FAU_GEN.1.1

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

a. Start-up and shutdown of the audit functions;

b. All auditable events for the [not specified] level of audit; and

c. [administrator login, administrator logout, self-test failures, peripheral device acceptance and rejections, [assignment: all administrative functions claimed in FMT_MOF.1 and FMT_SMF.1]]

4.1.1.2 FAU_GEN.1.2

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

a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [no other information].

Application Note

If a peripheral device is rejected due to its incompatibility with the peripheral interface, then this rejection need not be audited.

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this component.

TSS

The evaluator shall verify that the TSS describes the audit functionality including which events are audited, what information is saved in each record type, how the records are stored, the conditions in which audit records are overwritten, and the means by which the audit records may be read. Although the TOE may provide an interface for an administrator to view the audit records, this is not a requirement.

Guidance

The evaluator shall verify that the operational guidance provides instructions on how the audit logs can be viewed as well as any information needed to interpret the audit logs.

Test

The evaluator shall perform each of the auditable functions to succeed, and where possible, to fail. The evaluator shall use the means described in the TSS to access the audit records and verify that each of the events has been recorded, with all of the expected information.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.1 Security Audit of the TSS describes in detail the audit functions, both the RAM logs and the one-time programming (OTP) logs.

Guidance Evaluator Assessment:

[ADMIN] states in Administrator Configuration, "The product enables authorized administrators to download event log files and audit the product history as well as have access to advanced settings. This function is available only to authenticated administrators."

Also stated is that "Note: the log data may not be erased and log functions may not be disabled by users or administrators. RFD does not reset the administrator's password and username but deletes the additional users that the admin has created.

Test Evaluator Assessment:

1. Set up the TOE to enable administrator access per applicable TOE administrative guidance. Verify that the TOE is in factory default format.
2. Attempt to login to the TOE.
3. Log into the TOE using administrative credentials and password.
4. Connect a USB User Authentication (UA) device to the TOE.
5. Configure DPP settings to reject the UA device.
6. Exit initiate a self-test failure, and power down the TOE.
7. Log into the TOE using an administrative account and create a new administrator.
8. Perform a reset to factory defaults.
9. Attempt to log into the TOE using the new administrator. Verify it fails because the accounts are reset.
10. Log into the TOE using the default administrator account and attempt to change the default administrator account password.
11. Open the Critical RAM log
12. Verify the configure DPP action to reject the UA device from Step 5 is recorded in the log with a reliable timestamp.
13. Verify the self-test failure from Step 6 is recorded in the log with a reliable timestamp.
14. Verify the update to the whitelist/blacklist table from Step 5 is recorded in the log with a reliable timestamp.
15. Verify the reset to factory action from Step 8 is recorded in the log with a reliable timestamp.
16. Verify the default administrator password change from Step 10 is recorded in the log with a reliable timestamp.
17. Logout
18. Attempt to log into the TOE with an invalid username or invalid password.
19. Log into the TOE using an administrative account and create 2 new administrators.
20. Logout and Log into the TOE with one of the new administrator accounts. Then change the password of the new administrator account.
21. Perform a delete all accounts action.
22. Open the Non-critical RAM log.
23. Verify the administrator login failure(s) from Step 18 is recorded in the log with a reliable timestamp .
24. Verify the creation of administrator accounts from Step 19 are recorded in the log with a reliable timestamp .
25. Verify the password change of the newly creation administrator account from Step 20 is recorded in the log with a reliable timestamp .
26. Verify the account deletion from Step 21 is recorded in the log with a reliable timestamp .
27. Verify administrator logins are recorded in the log with a reliable timestamp .
28. Verify administrator logouts are recorded in the log with a reliable timestamp .
29. Verify the peripheral device acceptance from Step 4 is recorded in the log with a reliable timestamp .

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

4.2 User Data Protection (FDP)

4.2.1 FDP_CDS_EXT.1 Connected Displays Supported

4.2.1.1 FDP_CDS_EXT.1.1

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

Application Note

This SFR must be claimed if "switching can be initiated only through express user action" is chosen as a selection for FDP_SWI_EXT.1 in the PSD PP.

If "peripheral devices using a guard" is selected in FDP_SWI_EXT.2.2 (from the PSD PP), then "multiple connected displays" must be selected in FDP_CDS_EXT.1.1.

Evaluation Activity

Isolation Document

There are no Isolation Document EAs for this component.

TSS

The evaluator shall examine the TSS and verify that it describes how many connected displays may be supported at a time.

Guidance

The evaluator shall examine the operational user guidance and verify that it describes how many displays are supported by the TOE.

Test

There are no test EAs for this component beyond what the PSD PP requires.

Isolation Document Evaluator Assessment:

N A

TSS Evaluator Assessment:

Section 9.2.3.1 of the TSS states “The SK41PHU-4 device supports a single display. The DK42PHU-4, SX42PHU-4, SX82PHU-4, SC42DHU-4 and SC42PHU-4 devices support two displays.”

Guidance Evaluator Assessment:

Section 4.5 of the [CC_Supp] has a table (Table 2) that lists each device and the number of displays per device.

Test Evaluator Assessment:

NA

4.2.2 FDP_IPC_EXT.1 Internal Protocol Conversion

4.2.2.1 FDP_IPC_EXT.1.1

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

4.2.2.2 FDP_IPC_EXT.1.2

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

Application Note

This SFR must be claimed if "DisplayPort" is chosen as a selection for FDP_PDC_EXT.2.1/VI.

Evaluation Activity

Isolation Document

There are no Isolation Document EAs for this component.

TSS

The evaluator shall examine the TSS and verify that it describes how data DisplayPort data is converted.

Guidance

There are no guidance EAs for this component.

Test

Testing for this SFR is covered under FDP_APC_EXT.1 Test 3-VI.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.2.3 of the TSS discusses the video switching functionality in detail. In the discussion it states that "For DisplayPort connections, the TOE video function filters the AUX channel by converting it to I2C EDID only. DisplayPort video is converted into an HDMI video stream, and the I2C EDID lines connected to the emulated EDID EEPROM functions…".

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

NA

4.2.3 FDP_SWI_EXT.3 Tied Switching

4.2.3.1 FDP_SWI_EXT.3.1

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

Application Note

This SFR must be claimed if "switching can be initiated only through express user action" is chosen as a selection for FDP_SWI_EXT.1.1 in the PSD PP and if both "USB (keyboard)" and "USB (mouse)" are chosen as selections in FDP_PDC_EXT.2.1/KM.

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this SFR.

TSS

The evaluator shall verify that the TSS does not indicate that keyboard and mouse devices may be switched independently to different connected computers.

Guidance

The evaluator shall verify that the guidance does not describe how to switch the keyboard and mouse devices independently to different connected computers.

Test

The evaluator shall verify that the keyboard and mouse devices are always switched together to the same connected computer throughout testing in FDP_APC_EXT.1 in [MOD_KM_SD] section 2.1.3 above.

Tests for this SFR are performed in FDP_APC_EXT.1 test 1-KM in [MOD_KM_V1.0_SD] section 2.1.3 above.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.2.2.2 of the TSS discusses keyboard and mouse switching. In section 9.5 the TSS states “The TOE user switches between computers by pressing the corresponding front panel button on the device. The front panel button corresponding to the selected computer will illuminate.”

Guidance Evaluator Assessment:

The evaluator verified that guidance documents, [19959], [19961], [19969] and [20601] do not describe the keyboard and mouse switching independently to a different computer.

Test Evaluator Assessment:

NA

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

4.2.4.1 FDP_RIP.1.1/KM

The TSF shall ensure that any keyboard data in volatile memory is purged upon switching computers.

Application Note

This SFR must be claimed if "switching can be initiated only through express user action" is chosen as a selection for FDP_SWI_EXT.1.1 in the PSD PP and if "USB (keyboard)" is chosen as a selection in FDP_PDC_EXT.2.1/KM.

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this component.

TSS

The evaluator shall verify that the TSS indicates whether or not the TOE has user data buffers.

The evaluator shall verify that the TSS describes how all keyboard data stored in volatile memory is deleted upon switching computers.

Guidance

There are no guidance EAs for this component.

Test

There are no test EAs for this component.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.2.2.1 of the TSS states “The Static Random Access Memory (SRAM) in the host and device emulator circuitry stores USB Host stack parameters and up to the last 4 key codes. User data may be briefly retained; however, there are no data buffers. Data is erased during power off of the KVM, and when the user switches channels. When the TOE switches from one computer to another, the system controller 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.”

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

NA

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

4.2.5.1 FDP_SPR_EXT.1.1/DP

The TSF shall apply the following rules for the [DisplayPort] protocol:

- block the following video/display sub-protocols:

o [CEC,

o EDID from computer to display,

o HDCP,

o MCCS]

- allow the following video/display sub-protocols:

o [EDID from display to computer,

o HPD from display to computer,

o Link Training].

Application Note

The ST author must include this SFR if "DisplayPort" is selected in FDP_PDC_EXT.3.1/VI.

Evaluation Activity

Isolation Document

There are no Isolation Document EAs for this component.

TSS

The evaluator shall examine the TSS and verify that it describes that the various sub-protocols are allowed or blocked by the TOE as described by the SFR.

Guidance

There are no guidance EAs for this component.

Test

Testing for this SFR is covered under FDP_APC_EXT.1 Test 3-VI and Test 4-VI.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.2.3 of the TSS has a detailed discussion on the useable protocols by the display port.

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

NA

4.2.6 FDP_SPR_EXT.1/DVI-D Sub-Protocol Rules (DVI-D Protocol)

4.2.6.1 FDP_SPR_EXT.1.1/DVI-D

The TSF shall apply the following rules for the [DVI-D] protocol:

- block the following video/display sub-protocols:

o [ARC,

o CEC,

o EDID from computer to display,

o HDCP,

o HEAC,

o HEC,

o MCCS]

- allow the following video/display sub-protocols:

o [EDID from display to computer,

o HPD from display to computer].

Application Note

The ST author must include this SFR if "DVI-D" is selected in FDP_PDC_EXT.3.1/VI.

Evaluation Activity

Isolation Document

There are no Isolation Document EAs for this component.

TSS

The evaluator shall examine the TSS and verify that it describes that the various sub-protocols are allowed or blocked by the TOE as described by the SFR.

Guidance

There are no guidance EAs for this component.

Test

Testing for this SFR is covered under FDP_APC_EXT.1 Test 3-VI and Test 4-VI.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.2.3 of the TSS has a discussion on the useable protocols by the DVI-D port

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

NA

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

4.2.7.1 FDP_SPR_EXT.1.1/HDMI

The TSF shall apply the following rules for the [HDMI] protocol:

- block the following video/display sub-protocols:

o [ARC,

o CEC,

o EDID from computer to display,

o HDCP,

o HEAC,

o HEC,

o MCCS]

- allow the following video/display sub-protocols:

o [EDID from display to computer,

o HPD from display to computer].

Application Note

The ST author must include this SFR if "HDMI" is selected in FDP_PDC_EXT.3.1/VI.

Evaluation Activity

Isolation Document

There are no Isolation Document EAs for this component.

TSS

The evaluator shall examine the TSS and verify that it describes that the various sub-protocols are allowed or blocked by the TOE as described by the SFR.

Guidance

There are no guidance EAs for this component.

Test

Testing for this SFR is covered under FDP_APC_EXT.1 Test 3-VI and Test 4-VI.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.2.3 of the TSS has a discussion on the useable protocols by the HDMI port.

Guidance Evaluator Assessment:

NA

Test Evaluator Assessment:

NA

4.2.8 FDP_SWI_EXT.2 PSD Switching Methods

4.2.8.1 FDP_SWI_EXT.2.1

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

4.2.8.2 FDP_SWI_EXT.2.2

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

Application Note

This SFR must be claimed if “switching can be initiated only through express user action” is chosen as the selection for FDP_SWI_EXT.1.1.

If the TOE also claims conformance to the PP-Module for Video/Display Devices (Video Module) and if “peripheral devices using a guard” is selected here, the TOE must claim the selection-based requirement FDP_CDS_EXT.1 in the Video Module and select “multiple connected displays” in FDP_CDS_EXT.1.1.

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this component.

TSS

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.

If "peripheral devices using a guard" is selected, the evaluator shall verify that the TSS describes the implementation of the guard function, and verify that multiple, simultaneous express user action is required to switch between connected computers using connected peripheral devices.

Guidance

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.

If "peripheral devices using a guard" is selected, the evaluator shall verify that the user guidance describes the steps the user must take as required by the guard to switch between connected computers using a connected peripheral pointing device.

Test

[UA] Test performed in FDP_APC_EXT.1 above.

The evaluator shall ensure that switching is always initiated through express user action using the selected mechanisms throughout testing for FDP_APC_EXT.1 above.

Additional tests for this SFR are performed in FDP_APC_EXT.1 test 1-KM above.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.2.1 of the TSS states, “The user determines which host computer is to be connected to the peripherals by pressing a button on the TOE front panel or on the Auxiliary Front Panel. Switching can only be initiated through express user action.“

Matrix and combiner devices may be switched with peripheral devices using a guard. This is done by moving the mouse to the edge of the screen while pressing the left CTRL key.”

Guidance Evaluator Assessment:

The [19959], [19961], [19969] and the [20601] explain the device switching mechanisms. The [ADMIN] also has a “Warnings and Precautions” section which explains the limitations of the TOE.

Test Evaluator Assessment:

NA

4.2.9 FDP_TER_EXT.2 Session Termination of Removed Devices

4.2.9.1 FDP_TER_EXT.2.1

The TSF shall terminate an open session upon removal of the user authentication device.

Application Note

This SFR must be claimed if "external" is selected in FDP_PDC_EXT.4.1/UA.

Evaluation Activity

Isolation Document

There are no Isolation Document activities for this component.

TSS

The evaluator shall examine the TSS and verify that the TOE terminates an open session upon removal of the authentication device.

Guidance

The evaluator shall examine the guidance documentation and verify that the TOE terminates an open session upon removal of the authentication device.

Test

Testing for this component performed as part of FDP_APC_EXT.1 test 2-UA.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.2.4 of the TSS states "Following triggering of the anti-tampering function, following a failed self-test, or when the TOE is powered off, all user authentication device data paths are isolated through the peripheral multiplexer. These events effectively disconnect any open authentication session. Removal of the authentication device will also close the authentication session."

Guidance Evaluator Assessment:

The [CC_Supp] section 4.6 states "An open authentication device session is terminated on removal of the smartcard, authentication device, or when the device is switched to a different computer."

Test Evaluator Assessment:

NA

4.2.10 FDP_TER_EXT.3 Session Termination upon Switching

4.2.10.1 FDP_TER_EXT.3.1

The TSF shall terminate an open session upon switching to a different computer.

4.2.10.2 FDP_TER_EXT.3.2

The TSF shall reset the power to the user authentication device for at least one second upon switching to a different computer.

Application Note

This SFR must be claimed if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD-PP.

Evaluation Activity

Isolation Document

The evaluator shall examine the isolation document and verify that it describes how power is reset to the user authentication device upon switching.

TSS

The evaluator shall examine the TSS and verify that the TOE terminates an open session upon switching to a different computer.

Guidance

The evaluator shall examine the guidance documentation and verify that the TOE terminates an open session upon switching to a different computer.

Test

Testing for this component is performed as part of FDP_APC_EXT.1 test 2-UA.

Isolation Document Evaluator Assessment:

Section 3.9 of the [Isol] document states "When a user switches from one connected computer to another, the TOE resets the user authentication device through power supply switching, i.e. a temporary power dip. This is performed by High-side Power switches on the System Controller board that switch 5V power to the fUSB device jack. A load field-effect transistor (FET) shorts the supply voltage to the ground to quickly discharge any capacitance in the TOE or in the connected device to a level below 0.5V."

TSS Evaluator Assessment:

The TSS section 9.2.4 states "The TOE supports the use of a user authentication device with a feature called Freeze USB (fUSB). " and "When a user switches from one connected computer to another, the TOE resets the user authentication device through power supply switching, i.e. a temporary power dip. This is performed by High-side Power switches on the System Controller board that switch 5V power to the fUSB device jack. A load field-effect transistor (FET) shorts the supply voltage to the ground to quickly discharge any capacitance in the TOE or in the connected device to a level below 0.5V."

Guidance Evaluator Assessment:

The [CC_Supp] section 4.6 states "An open authentication device session is terminated on removal of the smartcard, authentication device, or when the device is switched to a different computer."

Test Evaluator Assessment:

NA

4.3 Identification and Authentication (FIA)

4.3.1 FIA_UAU.2 User Authentication Before Any Action

Note: This SFR is optional in the base PP. Inclusion of [MOD_KM] re-categorized it as selection-based. It shall be included in the TSF if 'configurable' is selected in FDP_FIL_EXT.1.1/KM.

Note: This SFR is optional in the base PP. Inclusion of [MOD_UA] re-categorized it as selection-based. It shall be included in the TSF if 'configurable' is selected in FDP_FIL_EXT.1.1/UA.

4.3.1.1 FIA_UAU.2.1

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

Application Note

This requirement expects that the authentication method(s) be described (e.g., logon credential, specially assigned key, etc.).

Evaluation Activity

This SFR is evaluated by the Evaluation Activities in FMT_MOF.1 below.

Evaluator Assessment:

NA

4.3.2 FIA_UID.2 User Identification Before Any Action

Note: This SFR is optional in the base PP. Inclusion of [MOD_KM] re-categorized it as selection-based. It shall be included in the TSF if 'configurable' is selected in FDP_FIL_EXT.1.1/KM.

Note: This SFR is optional in the base PP. Inclusion of [MOD_UA] re-categorized it as selection-based. It shall be included in the TSF if 'configurable' is selected in FDP_FIL_EXT.1.1/UA.

4.3.2.1 FIA_UID.2.1

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

Evaluation Activity

This SFR is evaluated by the Evaluation Activities in FMT_MOF.1 below.

Evaluator Assessment:

NA

4.4 Security Management (FMT)

4.4.1 FMT_MOF.1 Management of Security Functions Behavior

Note: This SFR is optional in the base PP. Inclusion of [MOD_KM] re-categorized it as selection-based. It shall be included in the TSF if 'configurable' is selected in FDP_FIL_EXT.1.1/KM.

Note: This SFR is optional in the base PP. Inclusion of [MOD_UA] re-categorized it as selection-based. It shall be included in the TSF if 'configurable' is selected in FDP_FIL_EXT.1.1/UA.

4.4.1.1 FMT_MOF.1.1

The TSF shall restrict the ability to [modify the behavior of] the functions [assignment: list of functions] to [the authorized administrators].

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this component.

TSS

The evaluator shall verify that the TSS describes the mechanism for preventing non-administrators from accessing the administrative functions stated above.

If the TSF provides multiple administrative roles, the evaluator shall verify that the authorized behavior for each separate administrative role is described.

The evaluator shall check the TSS to verify that it describes at least the following:

a) Administrator name limitations and syntax requirements;

b) Administrator password limitations and syntax requirements;

c) Restoring lost name or password;

d) Initial setting of administrator credentials;

e) Logon success, fail limitations, and logging; and

f) All functions identified in the above assignment.

Guidance

The evaluator shall check the user and administrative guidance to verify that the administrative functions described above are only available to identified administrators. If the TSF provides multiple administrative roles, the evaluator shall verify that the authorized behavior for each separate administrative role is described.

Test

Step 1: Set up the TOE to enable administrator access per applicable TOE administrative guidance. Verify that the TOE is in factory default format.

Step 2: Attempt to set the initial administrator user name and password.

Step 3: Logon as a valid administrator and perform all authorized administrative functions to assure the logon was successful.

Step 4: Log off from the TOE.

Step 5: Attempt to logon with an incorrect administrator name. Verify that the logon is failing as expected and that administrative functions are unavailable.

Step 6: Attempt to access administrative functions while there is no logged on administrator. Verify that all attempts fail.

Step 7: If the TOE provides multiple administrative roles, repeat this test for each defined role to ensure that the authorizations for each role are consistent with what is described in the operational guidance.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.3 of the TSS states that there is a single administrator account. Nine other accounts may be created. These additional accounts and associated passwords are removed when an RFD is performed. For these accounts, usernames must be between 8 and 11 characters in length and may be made up of uppercase and lowercase letters.

The primary administrator has a default password which is changed on first use. This account does not revert to default but maintains the administrator’s account when an RFD is performed. The administrator’s password must be between 8 and 15 characters in length and may contain uppercase letters, lowercase letters, numbers or any of the following special characters: ‘!’, ‘@’, ‘#’, ‘$’, ‘%’, ‘^’, ‘&’, ‘*’, ‘(’, ‘)’, ‘-’, or ‘_’. The password must contain at least one uppercase letter, one lowercase letter, one number and one special character.

Lost passwords are irrecoverable.

The user is locked out after three failed login attempts. The user may cycle the device power and try again. All password related events are logged.

Guidance Evaluator Assessment:

The administrator functions are only available to the administrator and are described in [ADMIN]. To perform administrator functions the administrator must be logged on. Users do not have access to administrator functions.

Test Evaluator Assessment:

Test 1

1. Set up the TOE to enable administrator access per applicable TOE administrative guidance. Verify that the TOE is in factory default format.
2. Attempt to set the initial administrator username and password.
3. Logon as a valid administrator and perform all authorized administrative functions to assure the logon was successful.
4. Log off from the TOE.
5. Attempt to logon with an incorrect administrative name and then attempt to logon with a correct administrator name using a wrong password.. Verify that the logon is failing as expected and that administrative functions are unavailable.
6. Attempt to access administrative functions while there is no logged-on administrator. Verify that all attempts fail.
7. If the TOE provides multiple administrative roles, repeat this test for each define role to ensure that the authorizations for each role are consistent with what is described in the operational guidance.

The evaluator confirmed that the administrative functions described in FMT_MOF.1.1 are only available to identified administrator.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

4.4.2 FMT_SMF.1 Specification of Management Functions

Note: This SFR is optional in the base PP. Inclusion of [MOD_KM] re-categorized it as selection-based. It shall be included in the TSF if ‘configurable’ is selected in FDP_FIL_EXT.1.1/KM.

Note: This SFR is optional in the base PP. Inclusion of [MOD_UA] re-categorized it as selection-based. It shall be included in the TSF if ‘configurable’ is selected in FDP_FIL_EXT.1.1/UA.

4.4.2.1 FMT_SMF.1.1

The TOE shall be capable of performing the following management functions: [assignment: list of management functions to be provided by the TSF].

Application Note

Supported management functions may depend on the PP-Modules that are claimed by the TOE alongside this PP. This could include Configurable Device Filtration (CDF) for one or more supported peripheral types not defined in this PP. A management function should also be included if the optional FDP_RIP_EXT.2.1 requirement is included which specifies that the TOE shall have a purge memory or restore factory defaults function accessible to the administrator.

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this component.

TSS

The evaluator shall check to ensure the TSS describes the management functions available to the administrators and user TOE configurations and how they are used by the TOE.

The evaluator shall check the TSS to verify that it describes at least the following:

a) Administrator name limitations and syntax requirements;

b) Administrator password limitations and syntax requirements;

c) Restoring lost name or password;

d) Initial setting of administrator credentials;

e) Logon success, fail limitations, and logging; and

f) All functions identified in the above assignment.

Guidance

The evaluator shall check that every management function mandated in the ST for this requirement is described in the operational user guidance and that the description contains the information required to perform the management duties associated with each management function.

Test

The evaluator shall test the TOE's ability to provide the management functions by configuring the TOE and testing each option assigned from above. The evaluator is expected to test these functions in all the ways in which the ST and guidance documentation state the configuration can be managed.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

A single administrator role is supported by the TOE. Administrators authenticate to the TOE by entering a username and password.

The primary administrator account cannot be deleted. The password remains the same and does not revert to the default when an RFD is performed.

The primary administrator has a default username and password that must be changed on first use.

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

Administrator passwords must be between 8 and 15 characters in length and may contain uppercase letters, lowercase letters, numbers or any of the following special characters: ‘!’, ‘@’, ‘#’, ‘$’, ‘%’, ‘^’, ‘&’, ‘*’, ‘(’, ‘)’, ‘-’, or ‘_’. The password must contain at least one uppercase letter, one lowercase letter, one number and one special character.

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

Once successfully authenticated, the administrator can use the console function to:

- Modify the CDF for authentication devices
- Manage administrator accounts (change password, create administrator account)
- Reset to factory defaults. This does not reset the primary administrator's username or password and does not reset the critical logs.

Guidance Evaluator Assessment:

The [CC_Supp] section 4.1 states "Instructions for users may be found in the Quick Installation Guides. Instructions for Administrators may be found in the HSL Administrator Guide." The [ADMIN] has the management functions described in the sections Administrator Setup/Log on, Terminal Mode Options and Terminal Mode Options - Explained.

Test Evaluator Assessment:

Test 1

The test case for this SFR is covered by FAU_GEN.1.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

4.4.3 FMT_SMR.1 Security Roles

Note: This SFR is optional in the base PP. Inclusion of [MOD_KM] re-categorized it as selection-based. It shall be included in the TSF if 'configurable' is selected in FDP_FIL_EXT.1.1/KM.

Note: This SFR is optional in the base PP. Inclusion of [MOD_UA] re-categorized it as selection-based. It shall be included in the TSF if 'configurable' is selected in FDP_FIL_EXT.1.1/UA.

4.4.3.1 FMT_SMR.1.1

The TSF shall maintain the roles [administrators].

4.4.3.2 FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Application Note

The intent of this SFR is to make clear the fact that the TSF is expected to provide some sort of controlled access to administrative functions such that ordinary users are not able to execute them without authorization. It does not mandate that the TSF provide a single administrative role named "administrator"; if multiple administrative roles with different authorizations are provided, then the behavior can be described in the ST and tested accordingly.

Evaluation Activity

Refer to the Evaluation Activities of FMT_MOF.1.1 above.

Evaluator Assessment:

NA done under FMT_MOF.1.1

4.5 Protection of the TSF (FPT)

4.5.1 FPT_STM.1 Reliable Time Stamps

Note: This SFR is optional in the base PP. Inclusion of [MOD_KM] re-categorized it as selection-based. It shall be included in the TSF if 'configurable' is selected in FDP_FIL_EXT.1.1/KM.

Note: This SFR is optional in the base PP. Inclusion of [MOD_UA] re-categorized it as selection-based. It shall be included in the TSF if 'configurable' is selected in FDP_FIL_EXT.1.1/UA.

4.5.1.1 FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

Application Note

Reliable time stamps are expected to be used with other TSF, e.g., for the generation of audit data, to allow the Administrator to investigate incidents by checking the order of events and to determine the actual local time when events occurred. The decision about the required level of accuracy of that information is up to the Administrator.

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this component.

TSS

The evaluator shall check to ensure the TSS describes how the TOE provides reliable timestamps.

Guidance

The evaluator shall check that the operational user guidance describes how the TOE provides reliable timestamps and if there are any management functions for configuring the time.

Test

The evaluator shall test the TOE's ability to provide time stamps. It is expected that this test be performed in conjunction with FAU_GEN.1.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

Section 9.4.3 of the TSS states that the devices each have a real-time clock powered by a battery and the time is set during production.

Guidance Evaluator Assessment:

Section 4.4 of the [CC_Supp] states "Each device includes a real-time clock powered by a battery. The time is set during production."

Test Evaluator Assessment:

The test case for this SFR is covered by FAU_GEN.1.

4.6 TOE Access (FTA)

4.6.1 FTA_CIN_EXT.1 Continuous Indications

This SFR is selection-based in the PSD PP. It remains selection-based when the TOE conforms to this PP Module. However, this PP-Module adds a trigger for its selection—specifically, if "multiple connected displays" is selected in FDP_CDS_EXT.1.1, then FTA_CIN_EXT.1 is applicable to the TOE and must be claimed.

The following SFR has a specific assignment, which is a mandatory selection if selecting "multiple connected displays" in FDP_CDS_EXT.1.1.

Additionally, the SFR is refined to specify an additional display mechanism in FTA_CIN_EXT.1.2

4.6.1.1 FTA_CIN_EXT.1.1

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

4.6.1.2 FTA_CIN_EXT.1.2

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

4.6.1.3 FTA_CIN_EXT.1.3

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

Application Note

This SFR must be claimed if "switching can be initiated only through express user action" is chosen as the selection for FDP_SWI_EXT.1.1.

FTA_CIN_EXT.1.3's selection of "multiple indicators which never display conflicting information" should be selected when the TOE has multiple indicators, and concerns TOEs with multiple authorized switching mechanisms that have distinct switching status indicators. Such indicators must never convey conflicting information to the user regarding the currently selected interface(s). In general, all indicators must always reflect the same status. It is permissible for the most recently used switching mechanism to reflect the current status while all other indicators to reflect no status. It is also permissible for a TOE that supports split control (i.e., different peripherals pointing to different computers) to have separate indicators for individual peripherals. Note however that a TOE that supports keyboard/mouse peripherals is not permitted to have the keyboard and mouse peripherals split in this manner, as per the requirements in the PP-Module for Keyboard/Mouse (KM) Devices.

If multiple products with single and multiple indicators are part of the TOE, then it is recommended that FTA_CIN_EXT.1.3 be iterated for each selection rather than do a different evaluation for each model.

Evaluation Activity

Isolation Document

There are no Isolation Document evaluation activities for this component.

TSS

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.

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.

Guidance

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. 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.

Test

Step 1: The evaluator shall configure the TOE and its operational environment in accordance with the operational user guidance.

Step 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.

Step 3: The evaluator shall repeat this process for every possible selected TOE configuration.

Step 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 powerup.

Step 5: The evaluator shall verify that the TOE selected computer indications are always on (i.e., continuous) and fully visible to the

TOE user.

Step 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.

Step 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.

Step 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.

[VI] Additional testing for this component is performed in test 1-VI of FDP_APC_EXT.1 in section 2.1.5 above.
Evaluator note: This is a reference to [MOD_VI_SD]

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

The TSS sections 9.2.1.3, 9.4.4 and 9.5 all describe the indicator (LED) behavior.

Guidance Evaluator Assessment:

The Quick Install Guides have a statement “By default, after product power-up, the active channel will be computer #1, indicated by the applicable front pane push button LED lit”. Section 4.3 of the [CC_Supp] states “Channel 1 is selected by default when the peripheral sharing device is started or reset.”

Test Evaluator Assessment:

Test 1

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.

The evaluator confirmed the TOE properly indicates which computer connection is active on TOE power up. 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.

Units Tested	**DK42PHU-4, SC42DHU-4**
Result	PASS

5 Security Assurance Requirement Activities

5.1 Development (ADV)

5.1.1 ADV_FSP.1 Basic Functional Specifications

Evaluation Activity

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 Assessment:

The [ST], [CC_Supp] and [ADMIN] were used to derive the verdicts for ADV_FSP.1. .The FDP_PDC_EXT.1.4 TSS Evaluation activity identifies the security relevant external interfaces of the TOE.

5.2 Guidance Documents (AGD)

5.2.1 AGD_OPE.1 Operational User Guidance

Evaluation Activity

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 Assessment:

The Guidance documents consist of Quick Installation Guides [19959], [19961], [19969] and [20601], as well as [CC_Supp] and [ADMIN]. These guides provide the information to assess the AGD_OPE.1 evaluation assessments. The guidance documents describe modes of operation, fail states, and procedures for the TOE's usage and operational environment.

5.2.2 AGD_PRE.1 Preparative Procedures

Evaluation Activity

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 Assessment:

The [CC_Supp] provides acceptance procedures and instructions for preparation of the operational environment. The Quick Installation Guidance's [19959], [19961], [19969] and [20601] provide clear installation procedures.

5.3 Life-Cycle Support (ALC)

5.3.1 ALC_CMC.1 Labeling of the TOE

Note

This component is targeted at identifying the TOE such that it can be distinguished from other products or versions from the same vendor and can be easily specified when being procured by an end user.

A label should consist of a "hard label" (e.g., stamped into the metal, paper label) or a "soft label" (e.g., electronically presented when queried).

The evaluator performs the CEM work units associated with ALC_CMC.1, as well as the Evaluation Activity specified below.

Evaluation Activity

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 Assessment:

The [ST] was used to determine the TOE identification and hence verdicts for ALC_CMC.1. The labeling on the guidance documents and nameplate on the underside of the TOE were consistent with the identification of the TOE.

5.3.2 ALC_CMS.1 TOE CM Coverage

Evaluation Activity

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 Assessment:

NA – covered under ALC_CMC.1

5.4 Tests (ATE)

5.4.1 ATE_IND Independent Testing - Conformance

Evaluation Activity

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 Assessment:

The evaluator tested the devices according to the tests in the PP and its modules. The setup was done according to the [19959], [19961] [20601], [CC_Supp] and the [ADMIN] guidance. The test case results were recorded in the [ETProcRes].

5.5 Vulnerability Analysis (AVA)

5.5.1 AVA_VAN.1 Vulnerability Survey

Evaluation Activity

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 Assessment:

The evaluator conducted a vulnerability assessment. The TOE is not connected to the Internet so no penetration tests were conducted. A vulnerability scan and search were conducted. This was recorded in the test plan [ETProcRes]. No vulnerabilities were found.