ASSURANCE ACTIVITY REPORT

Adder AS-4CR Multi-Domain Card Reader Firmware Version 40040-E7E7 Multi-Domain Card Reader

PREPARED BY
EWA-Canada, An Intertek Company

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

REPORT NO
2149-005-D007-3

DOCUMENT VERSION
Version 2.1

DATE
5 January, 2024

Contents

The Developer of the TOE:

Adder Technology 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 User Authentication Devices, 2019-07-19, Version 1.0

NIAP Technical Decisions

ITEM	TECHNICAL DECISION TITLE
TD0518	Typographical error in Dependency Table [PP_PSD_V4.0]
TD0583	FPT_PHP.3 modified for PSD remote controllers [PP_PSD_V4.0]
TD0593	Equivalency arguments for PSD [MOD_AI_V1.0], [MOD_AO_V1.0], [MOD_KM_V1.0], [MOD_UA_V1.0], [MOD_VI_V1.0]
TD0619	Test EAs for internal UA devices [MOD_UA_V1.0]
TD0804	Clarification regarding Extenders in PSD Evaluations [PP_PSD_V4.0]

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] Adder AS-4CR Multi-Domain Card Reader Firmware Version 40040-0E7Security Target, Version 1.4, 5 January 2024
- [CC_Supp] Adder AS-4CR Multi-Domain Card Reader Firmware Version 40040-0E7 Common Criteria Guidance Supplement, version 1.1, 8 May 2020
- [Isol] Adder AS-4CR Multi-Domain Card Reader Firmware Version 40040-0E7 Isolation Document, Version 1.3, 18 August 2020
- [QS-000044] ADDERView™ Secure 4-Port Card Reader, Quick Start, MAN-QS-000044_V0.1 RC2
- [ETProcRes] EVALUATION TEST PLAN, PROCEDURES AND TEST RESULTS FOR MULTI-DOMAIN CARD READER COMMON CRITERIA EVALUATION OF ADDER CFG_PSD-UA, version 2.1, 5 January 2024

1.2 *References*

- [PP_PSD_V4.0] Protection Profile for Peripheral Sharing Device, 2019-07-19, Version 4.0
- [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

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 [Isol] was reviewed. The document adequately describes the proper isolation whether the TOE is powered on or not.

TSS Evaluator Assessment:

The TSS discusses the conditions under which the TOE enters a failure state due to self-test failure in section 7.2.3 of the [ST]. “The TOE performs a self-test at initial start-up. The self-test runs independently and performs the following checks:

• Verification of the front panel push-buttons

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

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

Guidance Evaluator Assessment:

The [CC_Supp] Common Criteria Guidance Supplement explains the possible causes and the behavior of the device when in a fail state in section 4.1, it mentions that "A self test is performed at power up. Self test failures may be caused by an unexpected input at power up, or by a failure in the device integrity. A self test failure may also be an indication that the device has been tampered with."

Test Evaluator Assessment:

NA

2.1.2 FDP_APC_EXT.1/UA Active PSD Connections

2.1.2.1 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.

2.1.2.2 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.

2.1.2.3 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.

2.1.2.4 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	**AS-4CR**
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	**AS-4CR**
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	**AS-4CR**
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	**AS-4CR**

Result	PASS

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

2.1.3.1 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.

2.1.3.2 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.

2.1.3.3 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 (TD0619 Applied)

[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:

NA. The devices have fixed filtering.

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 not compatible with any of the TOE connectors, therefore this test is not applicable.

Units Tested	**AS-4CR**
Result	N/A

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 devices are treated correctly.

Units Tested	**AS-4CR**
Result	N/A

Test 3

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

Units Tested	**AS-4CR**
Result	PASS

2.1.4 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.

2.1.4.1 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.

2.1.4.2 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.

2.1.4.3 FDP_PDC_EXT.1.3

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

Evaluation activities are detailed below.

2.1.4.4 FDP_PDC_EXT.1.4

The TOE shall not have wireless interfaces.

Evaluation activities are detailed below.

2.1.4.5 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-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.

Isolation Document Evaluator Assessment:

NA

TSS Evaluator Assessment:

There are no wireless peripherals allowed in this configuration. The TSS section 7.1.2.1 states “The TOE does not support wireless connections of any type. The TSS describes all interfaces between the computers and the peripheral devices in sections 7.1 to 7.3. The TOE is compliant to the PSD PP and does not allow non-compliant devices.

Guidance Evaluator Assessment:

The [MAN-QS-000044] Quick Start Guide has 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	**AS-4CR**
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	**AS-4CR**
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	**AS-4CR**
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	**AS-4CR**
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	**AS-4CR**
Result	PASS

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

2.1.5.1 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.

2.1.5.2 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

2.1.6 FDP_PDC_EXT.4 Supported Authentication Device

2.1.6.1 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 7.1.2 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

2.1.7 FDP_PWR_EXT.1 Powered By Computer

2.1.7.1 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 7.1.2 of the TSS states that “Computer interfaces are isolated. Each computer interface uses

independent circuitry and power planes. There is no shared circuitry, and no shared logical functions."

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	**AS-4CR**
Result	PASS

2.1.8 FDP_SWI_EXT.1 PSD Switching

2.1.8.1 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 7.1.1 of the TSS states that "The user determines the host computer to be connected to the peripherals by pressing a button on the TOE front panel. The Light Emitting Diode (LED) above the front panel button of the selected computer is illuminated. Switching can only be initiated through express user action."

Guidance Evaluator Assessment:

The [MAN-QS-000044] Adder Quick Start Guide explains the device switching mechanisms.

Test Evaluator Assessment:

NA

2.1.9 FDP_RIP_EXT.1 Residual Information Protection

2.1.9.1 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

2.1.10 FDP_TER_EXT.1 Session Termination

2.1.10.1 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 7.1.2 of the TSS 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 4.3 of the [CC_Supp] states “An open authentication device session is terminated when the device is switched to a different computer.

Test Evaluator Assessment:

NA

2.1.11 FDP_UAI_EXT.1 User Authentication Isolation

2.1.11.1 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 2 indicates the authentication device isolation. Section 3.2 describes the UA device isolation.

TSS Evaluator Assessment:

Section 7.1.2 of the TSS says that “Computer interfaces are isolated. Each computer interface uses independent circuitry and power planes. There is no shared circuitry, and no shared logical functions”.

Guidance Evaluator Assessment:

The [MAN-QS-000044] Quick Start Guide and [Isol] section 2.3 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	**AS-4CR**
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	**AS-4CR**
Result	PASS

Test 3

NA

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_PHP.1 Passive Detection of Physical Attack

2.2.2.1 FPT_PHP_1.1

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

2.2.2.2 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 7.2.2 explains the anti-tamper mechanisms, the tamper evident seals. If a seal is removed, the word VOID appears to indicate the TOE has been tampered.

Guidance Evaluator Assessment:

The [MAN-QS-000044] Adder Quick Start 4-Port Card Reader Guide have a note on tamper. "Note: Holographic anti-tampering labels protect the product's enclosure, providing a clear visual indication if it has been opened or compromised."

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	**AS-4CR**
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	**AS-4CR**
Result	PASS

2.2.3 FPT_TST.1 TSF Testing

2.2.3.1 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]].

2.2.3.2 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].

2.2.3.3 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 7.3 of the TSS discusses the self-test and what it encompasses, which states "On power up and the successful completion of the self-test, or power up following reset and the successful completion of the self-test, the smartcard is connected to channel #1, and the LED above the corresponding push button will be illuminated"

Guidance Evaluator Assessment:

Section 4.1 of the [CC_Supp] Guidance Supplement states "A self test is performed at power up. Self test failures may be caused by an unexpected input at power up, or by a failure in the device integrity. A self test failure may also be an indication that the device has been tampered with.

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	**AS-4CR**
Result	PASS

2.2.4 FPT_TST_EXT.1 TSF Testing

2.2.4.1 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:

If a self-test were to fail, the TSS section 7.2.3 states that the following “If the self-test fails, the LEDs on the front panel blink and the device makes a clicking sound to indicate the failure. The TOE disables the PSD switching functionality, and remains in a disabled state until the self-test is rerun and passes”

Guidance Evaluator Assessment:

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	**AS-4CR**
Result	PASS

3 Optional Requirements Assurance Activities

4 Selection-Based Requirements Assurance Activities

4.1 *User Data Protection (FDP)*

4.1.1 FDP_TER_EXT.2 Session Termination of Removed Devices

4.1.1.1 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 7.1.2 of the TSS states “Following a failed self-test, or when the TOE is powered off, all user authentication device data paths are isolated through the 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] Guidance Supplement section 4.3 states “An open authentication device session is terminated when the device is switched to a different computer.”

Test Evaluator Assessment:

NA

4.1.2 FDP_TER_EXT.3 Session Termination upon Switching

4.1.2.1 FDP_TER_EXT.3.1

The TSF shall terminate an open session upon switching to a different computer.

4.1.2.2 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 3.2 of the [Isol] document states “the MDR TOE does not include any shared electronic components between the connected computers. The card can only be connected to a single channel at a time..”

TSS Evaluator Assessment:

The TSS section 7.1.2 states “When a user switches from one connected computer to another, the TOE resets the internal card reader through power supply switching, i.e. a temporary power dip. This is performed by High-side Power switches on the System Controller board that switches 5V power to the user authentication 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] Guidance Supplement section 4.3 states “An open authentication device session is terminated when the device is switched to a different computer.”

Test Evaluator Assessment:

NA

4.2 *TOE Access (FTA)*

4.2.1 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

4.2.1.1 FTA_CIN_EXT.1.1

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

4.2.1.2 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]].

4.2.1.3 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 7.2.3 and 7.3 all describe the indicator (LED) behavior.

Guidance Evaluator Assessment:

Section 4.2 of the [CC_Supp] states "Channel 1 is selected by default when the peripheral sharing device is started."

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	**AS-4CR**
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], TSS and [CC_Supp] 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 documentation consists of Quick Start Guides [MAN-QS-000044], and a [CC_Supp]. These provide the information to assess the AGD_OPE.1 assessments. The guidance documents describe modes of operation, fail states, and procedures for the TOE's usage and operational environment.

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 [CC_Supp] and the Quick Start Guides. The test cases were run successfully with pass verdicts recorded in the [ETProcRes]. The evaluation verdicts for the ATE class are in the ETR.

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 search was conducted. This was recorded in the test plan [ETProcRes]. No vulnerabilities were found.