Assurance Activity Report for
Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Peripheral Sharing Device

Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Peripheral Sharing Device Security Target
Version 1.12, October 20, 2021

Protection Profile for Peripheral Sharing Device, Version: 4.0
PP-Module for User Authentication Devices, Version 1.0

AAR Version 1.2, October 20, 2021

Evaluated by:

2400 Research Blvd, Suite 395
Rockville, MD 20850

Prepared for:

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

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

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

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

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

Common Criteria Version
Common Criteria Version 3.1 Revision 5

Common Evaluation Methodology Version
CEM Version 3.1 Revision 5

Contents

1 TOE Overview

The Vertiv Multi-Domain Smart Card Reader allows users to share a single card reader between a number of connected computers. Security features ensure isolation between computers and peripherals to prevent data leakage between connected systems. The TOE is a combined software and hardware TOE.

The following security features are provided by the Vertiv Peripheral Sharing Devices:

- Authentication Device
    - The TOE includes an authorized USB authentication device; the design inherently blocks all other devices.
- Hardware Anti-Tampering
    - Special holographic tampering evident labels on the product's enclosure provide a clear visual indication if the product has been opened or compromised.

2 Assurance Activities Identification

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

- PP-Module for User Authentication Devices, Version 1.0

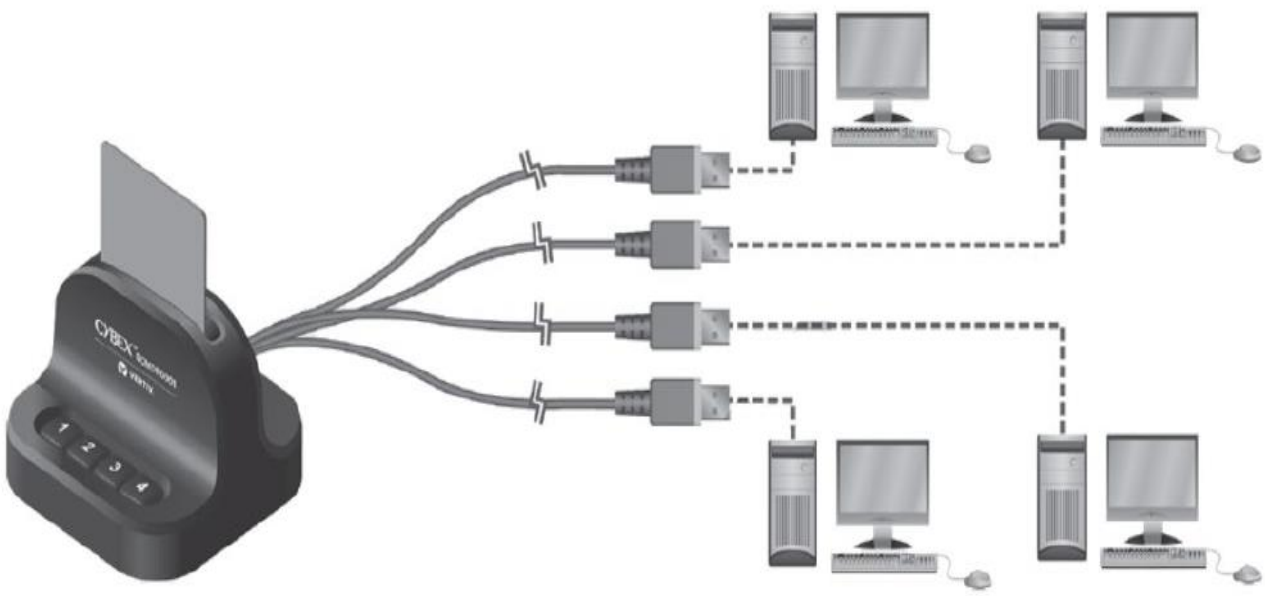
SFRs have been selected in accordance with PP-Configuration for Peripheral Sharing Device and User Authentication Devices, 19 July 2019 and on the selections within the PP and modules.

3 Test Bed Descriptions

3.1 Test Bed # 1

3.1.1 Visual Diagram

Below is a diagram of the components included in the test bed:



3.1.2 Test Equipment

The following equipment was used in the testing of the TOE:

Test Equipment
TELEDYNE LECROY USB-TMS2-M01-X USB Sniffer
Identiv SCR3310 USB UA Device with Power LED
Dell P2319H Monitor (High Resolution Monitor)
Dell Wired Keyboard KB216t
Keweisi USB Detector
Dell Wired Mouse M-UAR DEL 7

Computers

Name and Hardware	OS	Version	Function
Computer #1 HP ProDesk 600 G4	Windows 10	10.0.19041	Test Workstation – This computer will be connected to the Multi-Domain Card Reader and provide user authentication data when needed.
Computer #2 HP ProDesk 600 G4	Windows 10	10.0.19041	Test Workstation – This computer will be connected to the Multi-Domain Card Reader and provide user authentication data when needed.
Lab PC Dell Vostro Desktop	Windows 10	10.0.19041	Lab Workstation – This computer will be external to the TOE and be used in measuring the Multi-Domain Card Readers data output.

Software

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

3.1.3 Test Environment

The following test environment is in use throughout the testing process. The device will be tested using one lab workstation, and two test workstations. This will ensure throughout the testing process that at least two USB cables can be tested simultaneously. Throughout the testing the evaluator reconfigured the USB connections to the two test workstations to cover all possible combinations.

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

3.1.4 Test Time & Location

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

3.1.5 Configuration Information

The following device was tested:

Product: SCMDR0001

- Name: CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader
- Number of USB Cables: 4 Cables
- Security Peripherals: Common Access Card (CAC)

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

The following is a list of the documents consulted:

- Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Peripheral Sharing Devices Security Target, v1.12, October 20, 2021
- Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Peripheral Sharing Devices Isolation Document, Version 1.4, October 5, 2021
- Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Peripheral Sharing Devices Common Criteria Guidance Supplement, Version 1.4, October 5, 2021
- Test Report for Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Peripheral Sharing Device, version 1.2, October 20, 2021
- Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader SCMDR0001 Quick Installation Guide 590-2296-501 Rev. A

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

4.1.1 FDP_APC_EXT.1

4.1.1.1 FDP_APC_EXT.1 Isolation Document 1

Objective	The evaluator shall review the Isolation Documentation and Assessment as described in Appendix D of this PP and ensure that it adequately describes the isolation concepts and implementation in the TOE and why it can be relied upon to provide proper isolation between connected computers whether the TOE is powered on or powered off.
Evaluator Findings	The evaluator examined the [Isol]. Section 2.4 adequately describes the proper isolation whether the TOE is powered on or not. The 'Design Description' and 'Isolation Means Justification' sections describe how isolation is achieved. Section 2.3 titled 'Main Components in the Data Path' provides additional information on how isolation is achieved when the device is powered off. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.1.2 FDP_APC_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS describes the conditions under which the TOE enters a failure state.
Evaluator Findings	The evaluator examined section 7.2 titled 'Protection of the TSF' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that the TSS discusses the conditions under which the TOE enters a failure state. The device enters a failure state as a result of a self-test failure. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.1.3 FDP_APC_EXT.1 Guidance 1

Objective	The evaluator shall verify that the operational user guidance describes how a user knows when the TOE enters a failure state.
Evaluator Findings	The evaluator examined the [CC_Supp] to determine the verdict of this evaluation activity. The [CC_Supp] describes the possible error states, in section 4.3. The error state is indicated by sequential flashing of the Light Emitting Diodes and by a clicking noise. At this point, the device will be inoperable. It will not accept input from any smart card or pass data to any connected computer. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.2 FDP_APC_EXT.1/UA

4.1.2.1 FDP_APC_EXT.1/UA Isolation Document 1

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

4.1.2.2 FDP_APC_EXT.1/UA TSS 1

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

4.1.2.3 FDP_APC_EXT.1/UA Guidance 1

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

4.1.3 FDP_FIL_EXT.1/UA

4.1.3.1 FDP_FIL_EXT.1/UA Isolation Document 1

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

4.1.3.2 FDP_FIL_EXT.1/UA TSS 1

Objective	The evaluator shall examine the TSS and verify that it describes whether the PSD has configurable or fixed device filtering. [Conditional – If "configurable" is selected in FDP_FIL_EXT.1.1/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.
Evaluator Findings	The evaluator examined section 7.1.2 titled 'Smart Card Reader Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that the devices have fixed filtering. The device includes a standard USB smart card reader that complies with the USB Organization standard Chip Card Interface Device (CCID) Revision 1.1 and CCID Revision 1.0. The TOE provides fixed device filtering, allowing only the integrated smart card reader device to be used. There is no means of plugging in another peripheral device. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.3.3 FDP_FIL_EXT.1/UA Guidance 1

Objective	[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.
Evaluator Findings	The evaluator examined the security target to determine the verdict of this evaluation activity. The TOE contains "fixed" device filtering as per FDP_FIL_EXT.1/UA, therefore this conditional objective is not applicable. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.4 FDP_PDC_EXT.1

4.1.4.1 FDP_PDC_EXT.1 Isolation Document 1

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

4.1.4.2 FDP_PDC_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS describes the compatible devices for each peripheral port type supported by the TOE. The description must include sufficient detail to justify any PP-Modules that extend this PP and are claimed by the TOE (e.g., if the ST claims the Audio Input PP-Module, then the TSS shall reference one or more audio input devices as supported peripherals).

Evaluator Findings	The evaluator examined Section 7.1 titled 'User Data Protection' in the Security Target to determine the verdict of this evaluation activity. The compatible device type for each peripheral port type is described in the sections titled 'User Authentication Compatible Device Types'. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.4.3 FDP_PDC_EXT.1 TSS 2

Objective	The evaluator shall verify that the TSS describes the interfaces between the PSD and computers and the PSD and peripherals and ensure that the TOE does not contain wireless connections for these interfaces.
Evaluator Findings	The evaluator confirmed that the ST indicates that there are no wireless peripherals allowed in this configuration. The 'User Authentication Compatible Device Types' section 7.1.2.1 indicates that the TOE does not support a wireless connection to an authentication device. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.4.4 FDP_PDC_EXT.1 TSS 3

Objective	The evaluator shall verify that the list of peripheral devices and interfaces supported by the TOE does not include any prohibited peripheral devices or interface protocols specified in Appendix E.
Evaluator Findings	The evaluator examined Section 7.1 titled 'User Data Protection' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that Section 7.1.2.1 describes the allowed peripheral devices and protocols in 'User Authentication Compatible Device Types'. The TOE does not allow non-compliant devices. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.4.5 FDP_PDC_EXT.1 TSS 4

Objective	The evaluator shall verify that the TSS describes all external physical interfaces implemented by the TOE, and that there are no external interfaces that are not claimed by the TSF.
Evaluator Findings	The evaluator examined Section 7.1 titled 'User Data Protection' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section describes all physical interfaces to the peripheral devices in 'User Authentication Compatible Device Types'. The TOE is compliant to the PSD PP Appendix E and does describe any unclaimed external interfaces. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.4.6 FDP_PDC_EXT.1 Guidance 1

Objective	The evaluator shall verify that the operational user guidance provides clear direction for the connection of computers and peripheral devices to the TOE.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The evaluator examined the user guidance documentation. The [2296] provides clear instructions describing how to connect computers to the TOE. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.4.7 FDP_PDC_EXT.1 Guidance 2

Objective	The evaluator shall verify that the operational user guidance provides clear direction for the usage and connection of TOE interfaces, including general information for computer, power, and peripheral devices.
Evaluator Findings	The evaluator examined [CC_Supp] and [2296] to determine the verdict of this evaluation activity. The product guidance documents provide clear instructions on how to connect power and computers. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.4.8 FDP_PDC_EXT.1 Guidance 3

Objective	The evaluator shall determine if interfaces that receive or transmit data to or from the TOE present a risk that these interfaces could be misused to import or export user data.
Evaluator Findings	The evaluator examined [CC_Supp] to determine the verdict of this evaluation activity. Section 2, 3 and 4 provides additional instructions on usage, including environmental requirements required to alleviate the risk of data loss. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.4.9 FDP_PDC_EXT.1 Guidance 4

Objective	The evaluator shall verify that the operational user guidance describes the visual or auditory indications provided to a user when the TOE rejects the connection of a device.
Evaluator Findings	The evaluator examined [CC_Supp] and [2296] to determine the verdict of this evaluation activity. The TOE only allows the insertion of a single CAC smart card, thus no peripheral devices can be attached (and therefore rejected). When connected, the LED for the connected PC blinks continuously. When the card is inserted, the TOE beeps for one second and all LEDs turn off. When selecting a PC, the LED blinks for 5 seconds then turns solid. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.4.10 FDP_PDC_EXT.1 Guidance 1- UA

Objective	The evaluator shall verify that the operational user guidance describes devices authorized for use with the TOE in accordance with the authorized peripheral device connections.
Evaluator Findings	The evaluator examined [CC_Supp] and [2296] to determine the verdict of this evaluation activity. The product guidance documents clearly indicate that the TOE does not accept any peripheral device connections. It may be connected up to four PCs and supports insertion of a single CAC smart card. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.5 FDP_PDC_EXT.2/UA

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

4.1.6 FDP_PDC_EXT.4

4.1.6.1 FDP_PDC_EXT.4 Isolation Document 1

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

4.1.6.2 FDP_PDC_EXT.4 TSS 1

Objective	The evaluator shall examine the TSS and verify that it describes whether the PSD has internal or external authentication devices.
Evaluator Findings	The evaluator examined section 6.2.1.5 titled 'Supported Authentication Device' and 7.1.2.1 'User Authentication Compatible Device Types' in the Security Target to determine the verdict of this evaluation activity. The TOE contains an internal authentication device. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.6.3 FDP_PDC_EXT.4 TSS 2

Objective	Additional evaluation activities for STs that include the selection "external" are performed under FDP_PDC_EXT.1 in PSD PP.
Evaluator Findings	Not Applicable
Verdict	Pass

4.1.6.4 FDP_PDC_EXT.4 Guidance 1

Objective	There are no guidance evaluation activities for this component.

Evaluator Findings	Not Applicable
Verdict	Pass

4.1.7 FDP_PWR_EXT.1

4.1.7.1 FDP_PWR_EXT.1 Isolation Document 1

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

4.1.7.2 FDP_PWR_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS and verify that the connected computer does not power the TOE.
Evaluator Findings	The evaluator examined Section 7.1.2 titled 'Smart Card Reader Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that the TOE contains an independent power supply and is not dependent upon connected computers for power. When a user switches from one connected computer to another, the TOE resets the internal smart card reader through power supply switching, i.e. a temporary power dip. An on-board power switch controlled by the System Controller microcontroller unit (MCU) causes the power to drop on every channel switch. The TOE is provided with a power adapter. To power the TOE, one end is plugged into the TOE and the other is plugged into a power outlet. The TOE is not dependent upon the connected computers for power. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.7.3 FDP_PWR_EXT.1 Guidance 1

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

4.1.8 FDP_RIP_EXT.1

4.1.8.1 FDP_RIP_EXT.1 Isolation Document 1

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

Verdict	Pass

4.1.8.2 FDP_RIP_EXT.1 TSS 1

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

4.1.8.3 FDP_RIP_EXT.1 TSS 2

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

4.1.8.4 FDP_RIP_EXT.1 Guidance 1

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

4.1.9 FDP_SWI_EXT.1

4.1.9.1 FDP_SWI_EXT.1 Isolation Document 1

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

4.1.9.2 FDP_SWI_EXT.1 TSS 1

Objective	If the ST includes the selection the "TOE supports only one connected computer", the evaluator shall verify that the TSS indicates that the TOE supports only one connected computer.
Evaluator Findings	The evaluator examined FDP_SWI_EXT.1 in the 'Security Functional Requirements' section of the Security Target. The selection 'switching can be initiated only through express user action' has been made. Since 'TOE supports only one connected computer' is not selected, this evaluation activity is considered not applicable.
Verdict	Pass

4.1.9.3 FDP_SWI_EXT.1 TSS 2

Objective	If the ST includes the selection "switching can be initiated only through express user action", the evaluator shall verify that the TSS describes the TOE supported switching mechanisms and that those mechanisms can be initiated only through express user action.
Evaluator Findings	The evaluator examined the section titled 'TOE Overview' and the section titled 'System Controller' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that the 'TOE Overview' states that the Vertiv Multi-Domain Smart Card Reader (MDR) allow users to share a single card reader between a number of connected computers. The TSS has been written for multiple connected computers and explains how the user is able to conduct the switching. The 'System Controller' section describes the switching mechanism. All devices may be switched using the front panel buttons. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.9.4 FDP_SWI_EXT.1 Guidance 1

Objective	If the ST includes the selection "switching can be initiated only through express user action", the evaluator shall verify that the operational user guidance describes the TOE supported switching mechanisms.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The switching mechanisms are described in [CC_Supp] and [2296]. Each of these guides includes instructions on how the user performs switching. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.10 FDP_SWI_EXT.2

4.1.10.1 FDP_SWI_EXT.2 Isolation Document 1

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

4.1.10.2 FDP_SWI_EXT.2 TSS 1

Objective	The evaluator shall verify that the TSS describes the TOE supported switching mechanisms. The evaluator shall verify that the TSS does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms. The evaluator shall verify that the described switching mechanisms can be initiated only through express user action according to the selections.
Evaluator Findings	The evaluator examined the section titled 'System Controller' in the Security Target to determine the verdict of this evaluation activity. The TSS does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts The evaluator confirmed that all devices may be switched using the front panel. Switching can only be initiated through express user action. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.10.3 FDP_SWI_EXT.2 Guidance 1

Objective	The evaluator shall verify that the operational user guidance describes the TOE supported switching mechanisms. The evaluator shall verify that the operational user guidance does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms.
Evaluator Findings	The evaluator examined [2296] to determine the verdict of this evaluation activity. The switching mechanisms are described. The guide includes instructions on how the user performs switching. The evaluator also did not find any references to automatic port scanning, control through a connected computer, or keyboard shortcuts. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.11 FDP_TER_EXT.1

4.1.11.1 FDP_TER_EXT.1 Isolation Document 1

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

Verdict	Pass

4.1.11.2 FDP_TER_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS and verify that the TOE terminates an open session upon removal of the authentication element.
Evaluator Findings	The evaluator examined the section titled 'Smart Card Reader Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that removal of the authentication device will also close the authentication session. Once the authentication device is removed, the session is terminated. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.11.3 FDP_TER_EXT.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation and verify that the TOE terminates an open session upon removal of the authentication element.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Authentication Device Switching and Removal' Section 4.4 of the [CC_Supp] states "An open authentication device session is terminated when the device is switched to a different computer, or when the authentication element (i.e. smart card) is removed from the device. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.12 FDP_TER_EXT.2

4.1.12.1 FDP_TER_EXT.2 Isolation Document 1

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

4.1.12.2 FDP_TER_EXT.2 TSS 1

Objective	The evaluator shall examine the TSS and verify that the TOE terminates an open session upon removal of the authentication device.
Evaluator Findings	The evaluator examined the section titled 'Smart Card Reader Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that, 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. Based on these findings, this evaluation activity is considered satisfied.

Verdict	Pass

4.1.12.3 FDP_TER_EXT.2 Guidance 1

Objective	The evaluator shall examine the guidance documentation and verify that the TOE terminates an open session upon removal of the authentication device.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Authentication Device Switching and Removal' section 4.4 of the [CC_Supp] states " An open authentication device session is terminated when the device is switched to a different computer, or when the authentication element (i.e. smart card) is removed from the device." Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.13 FDP_TER_EXT.3

4.1.13.1 FDP_TER_EXT.3 Isolation Document 1

Objective	The evaluator shall examine the isolation document and verify that it describes how power is reset to the user authentication device upon switching.
Evaluator Findings	The evaluator examined the [Isol] section 3.2 titled 'Unauthorized Flow Designators R' to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that when a user switches from one connected computer to another, the TOE resets the internal smart card reader through power supply switching, i.e. a temporary power dip. An on-board power switch controlled by the System Controller microcontroller unit (MCU) causes the power to drop on every channel switch. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.13.2 FDP_TER_EXT.3 TSS 1

Objective	The evaluator shall examine the TSS and verify that the TOE terminates an open session upon switching to a different computer.
Evaluator Findings	The evaluator examined the section titled 'Smart Card Reader Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that 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. An on-board power switch controlled by the System Controller microcontroller unit (MCU) causes the power to drop on every channel switch. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.13.3 FDP_TER_EXT.3 Guidance 1

Objective	The evaluator shall examine the guidance documentation and verify that the TOE terminates an open session upon switching to a different computer.

Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Authentication Device Switching and Removal' section of the [CC_Supp] indicates that an open authentication device session is terminated when the device is switched to a different computer. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.14 FDP_UAI_EXT.1

4.1.14.1 FDP_UAI_EXT.1 Isolation Document 1

Objective	The evaluator shall examine the Isolation Documentation and verify that it describes how the TOE enforces user authentication isolation from other TOE USB functions.
Evaluator Findings	The evaluator examined the [Isol] to determine the verdict of this evaluation activity. Section 2 of the isolation document describes the main components and data flows. Power isolation is also described in this section. Section 3 describes unauthorized data flows and how isolation is provided. Interfaces are not shared and there are no wireless interfaces supported. Isolation is maintained with or without power applied to the TOE. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.14.2 FDP_UAI_EXT.1 TSS 1

Objective	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.
Evaluator Findings	The evaluator examined the section titled 'Smart Card Reader Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that authentication device functions use independent circuitry and power planes. There is no shared circuitry, and no shared logical functions. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.1.14.3 FDP_UAI_EXT.1 Guidance 1

Objective	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.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The [2296] provides a diagram showing a separate USB Type A cable interface which are to be attached to each connected computer. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

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

4.2.1 FPT_FLS_EXT.1(1)

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

4.2.2 FPT_NTA_EXT.1

4.2.2.1 FPT_NTA_EXT.1 Isolation Document 1

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

4.2.2.2 FPT_NTA_EXT.1 TSS 1

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

4.2.2.3 FPT_NTA_EXT.1 Guidance 1

Objective	The evaluator shall check the operational user guidance to ensure any configurations required to comply with this SFR are defined.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Secure Operation' Section 4 of [CC_Supp] provides a description of the configuration required. No additional configuration is required to comply with this SFR. The [2296] provides a diagram of the configuration required. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.2.3 FPT_PHP.1

4.2.3.1 FPT_PHP.1 Isolation Document 1

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

Verdict	Pass

4.2.3.2 FPT_PHP.1 TSS 1

Objective	The evaluator shall verify that the TSS indicates that the TOE provides unambiguous detection of physical tampering of the TOE enclosure and TOE remote controller (if applicable). The evaluator shall verify that the TSS provides information that describes how the TOE indicates that it has been tampered with.
Evaluator Findings	The evaluator examined the section titled 'Passive Anti-Tampering Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that the tamper evident seals are described in this section. Each device is fitted with holographic Tampering Evident Labels placed to cover both the top and bottom piece of the enclosure. If the label is removed, a honeycomb pattern appears on both the label and the product surface. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.2.3.3 FPT_PHP.1 Guidance 1

Objective	The evaluator shall verify that the operational user guidance describes the mechanism by which the TOE provides unambiguous detection of physical tampering and provides the user with instructions for verifying that the TOE has not been tampered with.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The [CC_Supp] Section 'Secure Acceptance Procedures' directs users to contact Technical Support if the enclosure appears to have been tampered with. The guidance documentation also states to ensure that the tamper-evident labels are intact prior to use. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.2.4 FPT_TST.1

4.2.4.1 FPT_TST.1 Isolation Document 1

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

4.2.4.2 FPT_TST.1 TSS 1

Objective	The evaluator shall verify that the TSS describes the self- tests that are performed on start up or on reset (if "upon reset button activation" is selected). The evaluator shall verify that the self-tests cover at least the following: a) a test of the user interface – in particular, tests of the user control mechanism (e.g., checking that the front panel push-buttons are not jammed); and

	b) if “active anti-tamper functionality” is selected, a test of any antitampering mechanism (e.g., checking that the backup battery is functional).
Evaluator Findings	The evaluator examined the section titled ‘TSF Testing’ in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section 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 Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.2.4.3 FPT_TST.1 TSS 2

Objective	The evaluator shall verify that the TSS describes how the TOE ensures a shutdown upon a self-test failure or a failed anti-tampering function, if present. If there are instances when a shutdown does not occur (e.g., a failure is deemed non-security relevant), those cases are identified and a rationale is provided explaining why the TOE’s ability to enforce its security policies is not affected.
Evaluator Findings	The evaluator examined the section titled ‘TSF Testing’ in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that 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. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.2.4.4 FPT_TST.1 TSS 3

Objective	The evaluator shall check the TSS to verify that it describes the TOE behavior in case of self-test failure. The evaluator shall verify that the described TOE behavior includes shutting down the PSD functionality once the failure is detected.
Evaluator Findings	The evaluator examined the section titled ‘TSF Testing’ in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that 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. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.2.4.5 FPT_TST.1 TSS 4

Objective	The evaluator shall examine the TSS to verify that it describes how users verify the integrity of the selections in FPT_TST.1.2 and FPT_TST.1.3. This method can include restarting the TOE, a dedicated self-test, or some other method.
Evaluator Findings	The evaluator examined the section titled 'TSF Testing' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that the TOE remains in a disabled state until the self-test is re-run and passes to clear the error. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.2.4.6 FPT_TST.1 Guidance 1

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

4.2.5 FPT_TST_EXT.1

4.2.5.1 FPT_TST_EXT.1 Isolation Document 1

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

4.2.5.2 FPT_TST_EXT.1 TSS 1

Objective	The evaluator shall check the TSS to verify that it describes the TOE behavior in case of self-test failure. The evaluator shall verify that the described TOE behavior includes shutting down the PSD functionality once the failure is detected.
Evaluator Findings	The evaluator examined the section titled 'TSF Testing' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section states that 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. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.2.5.3 FPT_TST_EXT.1 Guidance 1

Objective	The evaluator shall verify that the operational user guidance: a) describes how the results of self-tests are indicated to the user; b) provides the user with a clear indication of how to recognize a failed self-test; and c) details the appropriate actions to be completed in the event of a failed self-test.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Self Tests' section of the [CC_Supp] describes a self-test failure and explains what the operator has to do if there is a failure. A user may initiate a self-test by following the procedures outlined in Table 1 for the applicable device type. In the case of a self-test failure, users are directed to contact Vertiv Technical Support. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.2.5.4 FPT_TST_EXT.1 Guidance 2

Objective	The evaluator shall verify that the operational user guidance provides adequate information on TOE self-test failures, their causes, and their indications.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Self-Tests' and 'Error State' sections of the [CC_Supp] describes a self-test failure. The document indicates that self-test failures may be caused by an unexpected input at power up, or by a failure in the device integrity. Self-test failures are indicated by blinking LEDs and a clicking noise. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

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

4.3.1 FTA_CIN_EXT.1

4.3.1.1 FTA_CIN_EXT.1 Isolation Document 1

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

4.3.1.2 FTA_CIN_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS describes how the TOE behaves on power up and on reset, if applicable, regarding which computer interfaces are active, if any.
Evaluator Findings	The evaluator examined the section titled 'TOE Access' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that on power up or power up following reset, the smartcard is not connected to any channel. When the smart card reader becomes available, the LED indicators on the front panel flash to

	show the available connected computers. The user must select the connected computer to be used with the multi-domain smart card reader device. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.3.1.3 FTA_CIN_EXT.1 TSS 2

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

4.3.1.4 FTA_CIN_EXT.1 Guidance 1

Objective	The evaluator shall verify that the operational user guidance notes which computer connection is active on TOE power up or on recovery from reset, if applicable. If a reset option is available, use of this feature must be described in the operational user guidance.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The evaluator examined the [CC_Supp]. The 'Selected Channel at Startup' section indicates that no channel is selected by default when the peripheral sharing device is started or reset. When the smart card reader becomes available, the Light Emitting Diode (LED) indicators on the front panel flash to show the available connected computers. The user must select the connected computer to be used with the multi-domain smart card reader device. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

4.3.1.5 FTA_CIN_EXT.1 Guidance 2

Objective	The evaluator shall verify that the operational user guidance documents the behavior of all indicators when each switching mechanism is in use, and that no conflicting information is displayed by any indicators.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The evaluator examined [2296]. The guide describes the behavior of the TOE indicators. These documents provide a diagram and a description of the channel indicators and a description of the indicator behavior when the switching mechanism is in use. This behavior ensures that no conflicting information is displayed by the indicators. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5 Detailed Test Cases (Test Activities)

5.1 FDP_APC_EXT.1 Test 1

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1 – Test 1*
Objective	*[Conditional: Perform this test if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP]* 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
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Device Manager, Keweisi USB Detector, Fluke True RMS Digital Multimeter, Dell P2319H Monitor.
Test Objective Steps	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.
Expected Output	1. TOE is powered on. Computer #1 is selected. 2. Hardware information console indicates user authentication device. 3. User will repeat steps for each computer. 4. Evaluator will switch selected computers. 5. "Internal" was selected in FDP_PDC_EXT.4.1, therefore this step is non-applicable / pass. 6. The evaluator will verify that the hardware information console on the newly selected computer indicates the presence of the user authentication device. "Internal" was selected in FDP_PDC_EXT.4.1, therefore no DVM reading will be taken.
Pass/Fail Explanation	The evaluator confirms that the functionality of the TOE's UA switching methods is successful.
Unit Tested	SCMDR0001
Result	PASS

5.2 FDP_APC_EXT.1 Test 2

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

Objective	This test verifies correct data flows of a UA device during different power states of the selected computer.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Sniffer, Teledyne Lecroy USB Protocol Suite, USBlyzer, Device Manager, Dell P2319H Monitor.
Test Objective Steps	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. *[Conditional: Perform steps 5-6 if "external" is selected in FDP_PDC_EXT.4.1.]* 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. 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.] 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. 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.
Expected Output	1. USB sniffer setup correctly and USB analyzer software is open on the computer. 2. USB analyzer traffic is generated, and authentication session is active. 3. Authentication session is terminated. 4. USB analyzer traffic is generated, and authentication session is active. 5. "Internal" was selected in FDP_PDC_EXT.4.1, therefore this step is non-applicable/pass. 6. "Internal" was selected in FDP_PDC_EXT.4.1, therefore this step is non-applicable/pass. 7. Non-selected computers do not show UA device and no USB traffic is generated. 8. Authentication session will be terminated, hardware console does not recognize UA device, and no USB traffic is generated. 9. Authentication session is active and expected USB traffic is generated only on selected computer. 10. No USB traffic is generated on other USB analyzers. 11. No USB traffic is generated on non-selected computers. 12. No USB traffic is generated on non-selected computers. 13. No USB traffic is generated on non-selected computers. 14. No USB traffic is generated on non-selected computers. 15. Steps repeated while TOE is OFF and then in failure state. 16. Hardware console does not show device, no USB traffic is generated on non-selected computers. 17. Authentication session will be closed.
Pass/Fail Explanation	The evaluator confirms correct data flows of a UA device during different power states of the selected computer.
Unit Tested	SCMDR0001
Result	PASS

5.3 FDP_APC_EXT.1 Test 3

Item	***Data/Description***
Test ID	*FDP_APC_EXT.1 – Test 3*

Objective	*[Conditional: Perform this test if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP]* This test verifies no electric 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.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dr.Meter DC Power Supply, HSL USB Dummy Load, USBlyzer, Dell P2319H Monitor, Spliced USB Type-B Cable, USB Type-B to USB Type A adapter.
Test Objective Steps	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.]* 2. 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.
Expected Output	1. No USB traffic is generated on non-selected computers. 2. Replaced power supply with computer. 3. No USB traffic is generated on non-selected computers. 4. No USB traffic is generated on non-selected computers.
Pass/Fail Explanation	The evaluator confirms that no electric signals flow between connected computers when the TOE is powered on or off.
Unit Tested	SCMDR0001
Result	PASS

5.4 FDP_APC_EXT.1 Test 4

Item	***Data/Description***
Test ID	*FDP_APC_EXT.1 – Test 4*
Objective	This test verifies that the TOE does not send data to different computers connected to the same interface at different times. Repeat this test for each TOE 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.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, USBlyzer, Dell P2319H Monitor.
Test Objective Steps	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.
Expected Output	1. Only one computer is connected to the TOE and it is selected. 2. USB analyzer open and session ID recorded. 3. Authentication session open, Session ID recorded. 4. Sessions ID should be different from Step 2's session ID. 5. Authentication session open, Session ID recorded. 6. Sessions ID should be different from Step 2 and 4 session ID.
Pass/Fail Explanation	The evaluator confirms that the TOE does not send data to different computers connected to the same interface at different times.
Unit Tested	SCMDR0001
Result	PASS

5.5 FDP_PDC_EXT.1 Test 1

Item	***Data/Description***
Test ID	*FDP_PDC_EXT.1 – Test 1*
Objective	The evaluator shall check the TOE and its supplied cables and accessories to ensure that there are no external wired interfaces other than the computer interfaces, peripheral device interfaces, and power interfaces.
Test Equipment Used	N/A
Test Objective Step	1. Check the supplied cables and accessories to ensure there are no external wired interfaces other than the computer interfaces, peripheral device interfaces, and power interfaces.
Expected Output	1. Supplied cables and accessories contain no external wired interfaces other than the computer interfaces, peripheral device interfaces, and power interfaces.
Pass/Fail Explanation	The evaluator confirms that all supplied cables and accessories contain no external wired interfaces. This excludes computer interfaces, peripheral device interfaces, and power interfaces.
Unit Tested	SCMDR0001
Result	PASS

5.6 FDP_PDC_EXT.1 Test 2

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

Expected Output	1. The TOE does not support wireless interfaces.
Pass/Fail Explanation	The evaluator has checked the TOE for radio frequency certification information and verifies the TOE does not support wireless interfaces.
Unit Tested	SCMDR0001
Result	PASS

5.7 FDP_PDC_EXT.1 Test 3

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

	6. The TOE is powered off. The evaluator will connect an unauthorized USB device to USB hub. The evaluator will attempt to connected it to the TOE peripheral interface again. Since the TOE does not contain any USB input ports the evaluator will be unable to connect the device. 7. The evaluator will ensure the TOE is powered on. The device will be rejected as the TOE does not contain any USB input ports. 8. The evaluator disconnected the USB hub and attempted to connected it to the TOE peripheral interface. 9. The device will be rejected as the TOE does not contain any USB input ports. 10. The evaluator will ensure the TOE is powered on. The evaluator will attempt to connect a PS/2 device directly to the TOE peripheral interface. 11. The TOE is powered on; the device is rejected (The PS/2 device cannot be connected as the TOE contains no PS/2 ports). 12. The PS/2 device is already disconnected; attempted to connect it to the TOE peripheral interface. 13. The device is rejected (The PS/2 device cannot be connected as the TOE contains no PS/2 ports).
Pass/Fail Explanation	The evaluator confirms that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the Peripheral Device Connections (Appendix E). The evaluator confirms that the TOE does not possess any USB input or PS/2 input capabilities, therefore resulting in a rejection of those devices.
Units Tested	SCMDR0001
Result	PASS

5.8 FDP_PDC_EXT.1/UA - Test 1

Item	***Data/Description***
Test ID	*FDP_PDC_EXT.1 – Test 1*
Objective	*[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.
Test Equipment Used	N/A

Test Objective Steps	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.
Expected Output	N/A
Pass/Fail Explanation	"Internal" was selected in FDP_PDC_EXT.4.1, therefore this test case is non-applicable/pass.
Unit Tested	N/A
Result	N/A

5.9 FDP_PDC_EXT.1/UA Test 2

Item	***Data/Description***
Test ID	*FDP_PDC_EXT.1 – Test 2*
Objective	*[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.
Test Equipment Used	N/A
Test Objective Steps	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 is successfully connected on the connected computer. 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.
Expected Output	N/A
Pass/Fail Explanation	"Internal" was selected in FDP_PDC_EXT.4.1, therefore this test case is non-applicable / pass.
Unit Tested	N/A

Result	N/A

5.10 FDP_FIL_EXT.1/UA Test 1

Item	*Data/Description*
Test ID	*FDP_FIL_EXT.1 – Test 1*
Objective	Perform the test steps in FDP_PDC_EXT.1 with all devices on the PSD UA blacklist and verify that they are rejected as expected.
Test Equipment Used	N/A
Test Objective Steps	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.
Expected Output	1. The evaluator will ensure the TOE is powered off, hardware console application is running, and USB sniffer is connected to unauthorized device. 2. The evaluator will attempt to connect the unauthorized device via the USB sniffer to the TOE peripheral interface. 3. The TOE is powered on. The device is rejected as the TOE does not contain any USB inputs. 4. The evaluator will attempt to disconnect then reconnect the device. 5. The device will be rejected as the TOE does not contain any USB input ports. 6. The evaluator will repeat steps 1 – 5 with a USB hub connected between the USB device and the USB sniffer and verify that the device will be rejected.
Pass/Fail Explanation	The evaluator confirms that all devices on the PSD UA blacklist are rejected as expected. The TOE does not contain any user authentication peripheral interface ports in which unauthorized devices can be connected to, therefore resulting in a rejection of those devices.
Unit Tested	SCMDR0001
Result	PASS

5.11 FDP_FIL_EXT.1/UA Test 2

Item	*Data/Description*
Test ID	*FDP_FIL_EXT.1 – Test 2*
Objective	*[Conditional: Perform this only if "configurable" is selected in FDP_FIL_EXT.1.1/UA]* In the following steps the evaluator shall verify that whitelisted and blacklisted devices are treated correctly.
Test Equipment Used	N/A

Test Objective Steps	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.
Expected Output	N/A
Pass/Fail Explanation	"Fixed" has been selected in FDP_FIL_EXT.1.1/UA, therefore, this test is non-applicable / pass.
Unit Tested	N/A
Result	N/A

5.12 FDP_FIL_EXT.1/UA Test 3

Item	***Data/Description***
Test ID	*FDP_FIL_EXT.1 – Test 3*
Objective	*[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.
Test Equipment Used	N/A
Expected Output	N/A
Pass/Fail Explanation	The TOE does not contain any administrative command line interface in which the evaluator can examine the whitelist. The TSS states the authorized devices to be used with the TOE. Therefore, this test in non-applicable according to TQ #1198.
Unit Tested	N/A
Result	N/A

5.13 FDP_PWR_EXT.1 Test 1

Item	***Data/Description***
Test ID	*FDP_PWR_EXT.1 – Test 1*
Objective	The evaluator shall perform the following test for each connected computer.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Sniffer, Teledyne Lecroy USB Protocol Suite, Device Manager, Notepad, Dell P2319H Monitor.
Test Objective Steps	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.
Expected Output	1. The power source is disconnected from the TOE. 2. A USB sniffer is connected between a TOE UA computer interface and its computer. The TOE is attempted to be powered on. No user authentication

	device is present in the hardware console and no traffic is captured in the USB sniffer.
Pass/Fail Explanation	The evaluator confirms they performed the above test for each connected computer. No user authentication device is present, and no traffic was captured in the USB sniffer.
Unit Tested	SCMDR0001
Result	PASS

5.14 FDP_RIP_EXT.1 Test 1

Objective	There are no test Evaluation Activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.15 FDP_SWI_EXT.1 Test 1

Objective	There are no test Evaluation Activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.16 FDP_SWI_EXT.2 Test 1

Objective	There are no test Evaluation Activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.17 FDP_TER_EXT.1 Test 1

Objective	Testing for this component is performed as part of FDP_APC_EXT.1 test 2-UA.
Evaluator Findings	Not Applicable. See FDP_APC_EXT.1.
Verdict	Not Applicable

5.18 FDP_TER_EXT.2 Test 1

Objective	Testing for this component is performed as part of FDP_APC_EXT.1 test 2-UA.
Evaluator Findings	Not Applicable. See FDP_APC_EXT.1.
Verdict	Not Applicable

5.19 FDP_TER_EXT.3 Test 1

Objective	Testing for this component is performed as part of FDP_APC_EXT.1 test 2-UA.
Evaluator Findings	Not Applicable. See FDP_APC_EXT.1.
Verdict	Not Applicable

5.20 FDP_UAI_EXT.1 Test 1

Item	***Data/Description***
Test ID	*FDP_UAI_EXT.1 – Test 1*
Guidance	This test verifies that UA functionality is not sent to other USB interfaces. Perform this test for each computer interface.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Sniffer, Teledyne Lecroy USB Protocol Suite, Device Manager, Notepad, Dell P2319H Monitor.
Test Objective	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. *[Conditional: Perform steps 2 – 4 for each TOE USB peripheral interface other than UA.]* 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. *[Conditional: Perform steps 5 – 7 for each TOE USB computer interface other than UA.]* 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.
Expected Output	1. A display is connected directly to each computer. USB protocol, text editor and hardware information applications running on computer. An authorized device is connected. 2. USB sniffer connected to peripheral interface. 3. No USB traffic is captured. 4. Authentication session closed; USB sniffer disconnected. 5. USB sniffer connected to TOE USB computer interface. 6. No USB traffic is captured. 7. Authentication session closed; USB sniffer disconnected. 8. TOE is powered down. 9. No USB traffic is captured.
Pass/Fail Explanation	The evaluator confirms that user authentication functionality is not sent to other USB interfaces.

Unit Tested	SCMDR0001
Result	PASS

5.21 FDP_UAI_EXT.1 Test 2

Item	***Data/Description***
Test ID	*FDP_UAI_EXT.1 – Test 2*
Objective	*[Conditional: Perform this test only of 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.
Test Equipment Used	N/A
Test Objective Steps	1. Connect a KM device to the TOE KM peripheral interface. *[Conditional: Perform steps 2 – 3 for each TOE UA computer 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. *[Conditional: Perform steps 4 – 5 only if "external" is selected in FDP_PDC_EXT.4.1.]* 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.
Expected Output	N/A
Pass/Fail Explanation	The TOE does not support KM functionality; therefore, this test is non-applicable / pass.
Unit Tested	N/A
Result	N/A

5.22 FDP_UAI_EXT.1 Test 3

Item	***Data/Description***
Test ID	*FDP_UAI_EXT.1 – Test 3*
Objective	[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.
Test Equipment Used	N/A
Test Objective Steps	1. Connect a USB sniffer to the TOE UA computer interface. 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 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.]* 4. Disconnect the monitor.

	5. Disconnected the USB sniffer and connect it to the TOE UA peripheral device interface. 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. 7. Play a video on the selected computer and verify that no traffic is sent and captured on the USB sniffer.
Expected Output	N/A
Pass/Fail Explanation	The TOE does not support video functionality and "USB Type-C with DisplayPort as alternate function" is not selected in FDP_PDC_EXT.3.1/VI in MOD_VI_V1.0.] Therefore, this test is non-applicable / pass.
Unit Tested	N/A
Result	N/A

5.23 FPT_NTA_EXT.1 Test 1

Objective	There are no test Evaluation Activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.24 FPT_PHP.1 Test 1

Item	***Data/Description***
Test ID	*FPT_PHP.1 – Test 1*
Objective	The evaluator shall verify, for each tamper evident seal or label affixed to the TOE encloser and TOE remote controller, that any attempts to open the enclosure or remove the seal results in the seal being damaged in a manner that is consistent with the operational user guidance.
Test Equipment Used	N/A
Test Objective Step	1. Removed the tamper evident seals from the TOE.
Expected Output	1. Removal of tamper evident seals results in seals being damaged irreversibly.
Pass/Fail Explanation	The evaluator confirms that any attempt to open the enclosure or remove the seal results in the seal being damaged in a manner that is consistent with the operational user guidance.
Unit Tested	SCMDR0001
Result	PASS

5.25 FPT_PHP.1 Test 2

Item	***Data/Description***
Test ID	*FPT_PHP.1 – Test 2*
Objective	The evaluator shall verify that it is not possible to administratively disable or otherwise prevent the display of any tampering indicators.
Test Equipment Used	N/A
Test Objective Step	1. Attempt to remove the tamper evident seals from the TOE without damaging the tampering indicators.

Expected Output	1. The tampering indicators will be damaged and clearly display that the TOE has been tampered with.
Pass/Fail Explanation	The evaluator confirms that it is not possible to administratively disable or otherwise prevent the display of any tampering indicators.
Unit Tested	SCMDR0001
Result	PASS

5.26 FPT_TST.1 Test 1

Item	***Data/Description***
Test ID	*FPT_TST.1 – Test 1*
Objective	The evaluator shall trigger the conditions specified in the TSS that are used to initiate TSF self-testing and verify that successful completion of the self-tests can be determined by following the corresponding steps in operational guidance.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Objective Steps	1. The TOE must be powered off, ensure the power cable is removed from the TOE before proceeding. 2. The evaluator will insert a smart card into the TOE and will connect the power cable to the TOE. The evaluator will observe the TOE performs a start-up self-test diagnostic for the following criteria: • Verification of the front panel push buttons • Verification of the integrity of the microcontroller firmware • Verification of computer port isolation 3. Upon completion of the self-testing diagnostic the TOE will power on into operational mode and the LED indicators on the front panel will flash to show the available connected computers.
Expected Output	1. The TOE will be powered off, the power cable is removed from the TOE before proceeding. 2. The evaluator will insert a smart card into the TOE and will connect the power cable to the TOE. The evaluator will observe the TOE performs a start-up self-test diagnostic for the following criteria: • Verification of the front panel push buttons • Verification of the integrity of the microcontroller firmware • Verification of computer port isolation 3. Upon completion of the self-testing diagnostic the TOE will power on into operational mode and the LED indicators on the front panel will flash to show the available connected computers.
Pass/Fail Explanation	The evaluator confirms that that successful completion of the self-tests can be determined by following the corresponding steps in operational guidance.
Unit Tested	SCMDR0001
Result	PASS

5.27 FPT_TST_EXT.1 Test 1

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

Objective	The evaluator shall cause a TOE self-test failure and verify that the TOE responds by disabling normal functions and provides proper indications to the user.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Objective Steps	1. The TOE must be powered off, ensure the power cable is removed from the TOE before proceeding. 2. Firmly press the computer #1 front panel 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 input from any smart card is received and no data is passed to any connected computer while the TOE is in self-test failure state.
Expected Output	1. TOE will be powered off, cable unplugged from back of TOE. 2. The evaluator will firmly press the computer #1 front panel button on the TOE while simultaneously plugging in the power cable. The unit will 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 will remain inoperable. 3. The evaluator will ensure no input from any smart card is received and no data is passed to any connected computer while the TOE is in self-test failure state.
Pass/Fail Explanation	The evaluator confirms that the TOE does preform a self-test failure and that the TOE responds by disabling normal functions and provides proper indications to the user.
Unit Tested	SCMDR0001
Result	PASS

5.28 FTA_CIN_EXT.1 Test 1

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

	6. [Conditional] If the TOE allows peripherals to have active interfaces with different computers at the same time, the evaluator shall verify that each permutation has its own selection indications. 7. [Conditional] If "*a screen with dimming function*" is selected, the evaluator shall verify that indications are visible at minimum brightness settings in standard room illumination conditions. 8. [Conditional] If "*multiple indicators which never display conflicting information*" is selected, the evaluator shall verify that either all indicators reflect the same status at all times, or the indicator for the most recently used switching mechanism displays the correct switching status and that all other indicators display the correct status or no status
Expected Output	1. The TOE and its operational environment have been configured in accordance with the operational user guidance. 2. A computer will be selected, then the TOE will be powered down. The TOE will then be powered up and the evaluator will verify that the expected selected computer is indicated in accordance with the TSS and that the connection is active. 3. This process will be repeated for every possible selected TOE configuration. 4. This process will be repeated for every possible TOE configuration using the reset function rather than power-down and power-up. 5. The selected computer indications on the TOE are always on and fully visible to the TOE user. 6. The TOE shall allow peripheral to have active indications with different computers at the same time. 7. "*a screen with dimming function*" was not selected, therefore this step is non-applicable. 8. "*multiple indicators which never display conflicting information*" was not selected, therefore this step is non-applicable.
Pass/Fail Explanation	The evaluator confirms the TOE properly indicates which computer connection is active on TOE power up. The evaluator also verifies the behavior of all indicators when each switching mechanism is in use, and that no conflicting information is displayed by any indicators.
Unit Tested	SCMDR0001
Result	PASS

6 Security Assurance Requirements

6.1 ADV_FSP.1 Basic Functional Specification

6.1.1 ADV_FSP.1

6.1.1.1 ADV_FSP.1 Activity 1

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

6.2 AGD_OPE.1 Operational User Guidance

6.2.1 AGD_OPE.1

6.2.1.1 AGD_OPE.1 Activity 1

Objective	The operational user guidance does not have to be contained in a single document. Guidance to users and Administrators can be spread among documents or web pages. The developer should review the Evaluation Activities contained in Section 5.2 of this PP to ascertain the specifics of the guidance for which the evaluator will be checking. This will provide the necessary information for the preparation of acceptable guidance.
Evaluator Findings	The evaluator examined the guidance documents to perform this evaluation. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

6.3 AGD_PRE.1 Preparative Procedures

6.3.1 AGD_PRE.1

6.3.1.1 AGD_PRE.1 Activity 1

Objective	As with the operational user guidance, the developer should look to the Evaluation Activities contained in Section 5.2 of this PP to determine the required content with respect to preparative procedures.
Evaluator Findings	The evaluator examined the guidance documents to perform this evaluation. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

6.4 ALC Assurance Activities

6.4.1 ALC_CMC.1

6.4.1.1 ALC_CMC.1 Activity 1

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

6.4.2 ALC_CMS.1

6.4.2.1 ALC_CMS.1 Activity 1

Objective	Given the scope of the TOE and its associated evaluation evidence requirements, this component’s Evaluation Activities are covered by the Evaluation Activities listed for ALC_CMC.1.
Evaluator Findings	Not Applicable
Verdict	Pass

6.5 ATE_IND.1 Independent Testing – Conformance

6.5.1 ATE_IND.1

6.5.1.1 ATE_IND.1 Activity 1

Objective	The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the CEM and the body of this PP’s Evaluation Activities. While it is not necessary to have one test case per test listed in an Evaluation Activity, the evaluator must document in the test plan that each applicable testing requirement in the PP is covered. The test plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary. The test plan describes the composition of each platform to be tested and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluator is expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test equipment or tools. For each piece of equipment or tool, an argument (not just an

	assertion) should be provided that the equipment or tool will not adversely affect the performance of the functionality by the TOE and its platform. The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.
Evaluator Findings	The evaluator created a test plan and executed all the tests in the test plan. The results of all the testing are included in the test plan. Based on this document, this evaluation activity is considered satisfied.
Verdict	Pass

6.6 AVA_VAN.1 Vulnerability Survey

6.6.1 AVA_VAN.1

6.6.1.1 AVA_VAN.1 Activity 1

Objective	As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in peripheral sharing devices and the implemented communication protocols in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated.
Evaluator Findings	The evaluators documented their analysis and testing of potential vulnerabilities with respect to this requirement. Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included several combinations of the following words Vertiv, Cybex, SCMDR0001, Firmware Version 40040-0E7, Multi-Domain Smart Card Reader, NAK transaction and STMicroelectronics 32-Bit to ensure sufficient coverage under AVA. The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below. • National Vulnerability Database: https://nvd.nist.gov/vuln/search • Vertiv Support: https://www.vertiv.com/en-ca/support/ • Common Vulnerabilities and Exposures: https://google.com The search was performed on October 6, 2021. The evaluation team found no vulnerabilities were applicable to the TOE version or hardware. Based on these findings, this evaluation activity is considered satisfied.

Verdict	Pass

7 Conclusion

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

8 Evaluation Evidence

- Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Peripheral Sharing Devices Security Target, v1.12, October 20, 2021
- Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Peripheral Sharing Devices Isolation Document, Version 1.4, October 5, 2021
- Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Peripheral Sharing Devices Common Criteria Guidance Supplement, Version 1.4, October 5, 2021
- Test Report for Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Peripheral Sharing Device, version 1.2, October 20, 2021
- Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader SCMDR0001 Quick Installation Guide 590-2296-501 Rev. A

9 References

[PP_PSD_V4.0] Protection Profile for Peripheral Sharing Device, July 19, 2019
[MOD_UA_V1.0] PP-Module for User Authentication Devices, July 19, 2019
[CFG_PSD_UA_v1.0] PP-Configuration for Peripheral Sharing Device, User Authentication Devices, July 19, 2019

End of Document