Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader

Firmware Version 40040-0E7

Security Target

Doc No: 2149-001-D102C5
Version: 1.12
20 October 2021

Vertiv IT Systems
1050 Dearborn Dr,
Columbus, OH 43085

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

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the Target of Evaluation (TOE), the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

Section 1, ST Introduction, provides the Security Target reference, the Target of Evaluation reference, the TOE overview and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria, Protection Profile (PP) and PP Modules.

Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition.

Section 5, Extended Components Definition, defines the extended components which are then detailed in Section 6.

Section 6, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the IT environment.

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

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

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

1.2 SECURITY TARGET REFERENCE

ST Title:	Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Security Target
ST Version:	1.12
ST Date:	20 October 2021

1.3 TOE REFERENCE

TOE Identification: Vertiv CYBEX™ SCMDR0001 Multi-Domain Card Reader Firmware Version 40040-0E7

TOE Developer: Vertiv IT Systems

TOE Type: Peripheral Sharing Device (Other Devices and Systems)

1.4 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 following security features are provided by the Vertiv Multi-Domain Smart Card Reader:

- 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

The TOE is a combined software and hardware TOE.

1.4.1 TOE Environment

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

Component	Description
Connected Computers	1-4 General purpose computers
Smartcard	General purpose smartcard

Table 1 – Multi-Domain Smart Card Reader Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

1.5.1 Evaluated Configuration

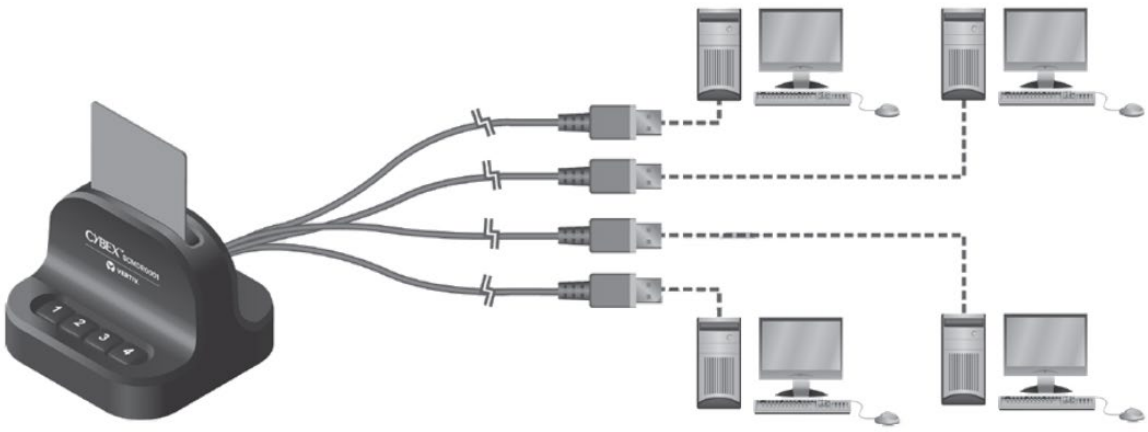


Figure 1 – Multi-Domain Smart Card Reader Evaluated Configuration

The Multi-Domain Smart Card Reader (MDR) is connected to up to four computers, and is used with a smart card.

1.5.2 Physical Scope

The TOE consists of the device shown in Table 2.

Family	Family Description	Part Number	Model	Tamper Evident labels
Multi-Domain Smart Card Reader	Switchable authentication peripheral device. This device is intended to support switching of Common Access Card (CAC) peripherals only.	CGA19217	SCMDR0001	Yes

Table 2 – TOE Device

1.5.2.1 TOE Delivery

The TOE is delivered to the customer via a trusted carrier, such as Fed-Ex, that provides a tracking service for all shipments.

1.5.2.2 TOE Guidance

The TOE includes the following guidance documentation:

- CYBEX™ SECURE MULT-DOMAIN SMART CARD READER, 590-2296-501 Rev. A

Guidance may be downloaded from the Vertiv website (www.vertiv.com) in .pdf format.

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

- Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Common Criteria Guidance Supplement, Version 1.4

1.5.3 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security functional classes described in Section 6. Table 3 summarizes the logical scope of the TOE.

Functional Classes	Description
User Data Protection	The TOE provides secure isolation between connected computers and a smartcard.
Protection of the TSF[1]	The TOE ensures a secure state in the case of failure, provides only restricted access, and performs self-testing. The TOE provides passive detection of physical attack.
TOE Access	The TOE provides a continuous indication of which computer is currently selected.

Table 3 – Logical Scope of the TOE

[1] TOE Security Functionality

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

As follows:

- CC Part 2 extended
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 has been taken into account.

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

This ST claims exact conformance with the National Information Assurance Partnership (NIAP) PP-Configuration for Peripheral Sharing Device and User Authentication Devices [CFG_PSD-UA_V1.0], which references the Protection Profile for Peripheral Sharing Device Version 4.0 [PP_PSD_V4.0], and the PP-Module for User Authentication Devices, Version 1.0 [MOD_UA_V1.0]. The Technical Decision in Table 4 applies to the PP and the module and has been accounted for in the ST and in the evaluation.

Technical Decision	PP or Module
TD0518	[PP_PSD_V4.0]
TD0583	[PP_PSD_V4.0]
TD0593	[MOD_UA_V1.0]

Table 4 – Applicable Technical Decisions

2.3 PACKAGE CLAIM

This Security Target does not claim conformance with any package.

2.4 MODULE CLAIM

The following PP-Module is specified in a PP-Configuration with this PP:

- PP-Module for User Authentication Devices, Version 1.0

2.5 CONFORMANCE RATIONALE

The TOE Multi-Domain Smart Card Reader is consistent with the Compliant Targets of Evaluation described in the [PP_PSD_V4.0] and in the PP-Module for User Authentication Devices [MOD_UA_V1.0], and with the PP-Configuration for Peripheral Sharing Device and User Authentication Devices [CFG_PSD-UA_V1.0].

The security problem definition, statement of security objectives and statement of security requirements in this ST conform exactly to the security problem definition, statement of security objectives and statement of security requirements contained in [PP_PSD_V4.0] and [MOD_UA_V1.0].

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

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

Threat	Description
T.DATA_LEAK	A connection via the PSD between one or more computers may allow unauthorized data flow through the PSD or its connected peripherals.
T.SIGNAL_LEAK	A connection via the PSD between one or more computers may allow unauthorized data flow through bit-by-bit signaling.
T.RESIDUAL_LEAK	A PSD may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer.
T.UNINTENDED_USE	A PSD may connect the user to a computer other than the one to which the user intended to connect.
T.UNAUTHORIZED_DEVICES	The use of an unauthorized peripheral device with a specific PSD peripheral port may allow unauthorized data flows between connected devices or enable an attack on the PSD or its connected computers.
T.LOGICAL_TAMPER	An attached device (computer or peripheral) with malware, or otherwise under the control of a malicious user, could modify or overwrite code or data stored in the PSD's volatile or non-volatile memory to allow unauthorized information flows.
T.PHYSICAL_TAMPER	A malicious user or human agent could physically modify the PSD to allow unauthorized information flows.
T.REPLACEMENT	A malicious human agent could replace the PSD during shipping, storage, or use with an alternate device that does not enforce the PSD security policies.
T.FAILED	Detectable failure of a PSD may cause an unauthorized information flow or weakening of PSD security functions.

Table 5 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

There are no Organizational Security Policies applicable to this TOE.

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 6.

Assumptions	Description
A.NO_TEMPEST	Computers and peripheral devices connected to the PSD are not TEMPEST approved.
A.PHYSICAL	The environment provides physical security commensurate with the value of the TOE and the data it processes and contains.
A.NO_WIRELESS_DEVICES	The environment includes no wireless peripheral devices.
A.TRUSTED_ADMIN	PSD Administrators and users are trusted to follow and apply all guidance in a trusted manner.
A.TRUSTED_CONFIG	Personnel configuring the PSD and its operational environment follow the applicable security configuration guidance.
A.USER_ALLOWED_ACCESS	All PSD users are allowed to interact with all connected computers. It is not the role of the PSD to prevent or otherwise control user access to connected computers. Computers or their connected network shall have the required means to authenticate the user and to control access to their various resources.

Table 6 – Assumptions

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address the security concerns and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats may be addressed by the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the environment

4.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describes the security objectives that are to be addressed by the TOE, and traces each Security Functional Requirement (SFR) back to a security objective of the TOE.

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td>O.COMPUTER
_INTERFACE
_ISOLATION</td><td>The PSD shall prevent unauthorized data flow to ensure that the PSD and its connected peripheral devices cannot be exploited in an attempt to leak data. The TOE-Computer interface shall be isolated from all other PSD-Computer interfaces while TOE is powered.
Addressed by:<table><tr><td>MOD_UA</td><td>FDP_APC_EXT.1/UA, FDP_FIL_EXT.1/UA, FDP_PDC_EXT.1, FDP_PDC_EXT.2/UA, FDP_PDC_EXT.4, FDP_PWR_EXT.1, FDP_SWI_EXT.2</td></tr></table></td></tr>
<tr><td>O.COMPUTER
_INTERFACE
_ISOLATION
_TOE_UNPOWERED</td><td>The PSD shall not allow data to transit a PSD-Computer interface while the PSD is unpowered.
Addressed by:<table><tr><td>MOD_UA</td><td>FDP_APC_EXT.1/UA, FDP_FIL_EXT.1/UA, FDP_PDC_EXT.1, FDP_PDC_EXT.2/UA, FDP_PDC_EXT.4, FDP_PWR_EXT.1, FDP_SWI_EXT.2</td></tr></table></td></tr>
<tr><td>O.USER_DATA
_ISOLATION</td><td>The PSD shall route user data, such as keyboard entries, only to the computer selected by the user. The PSD shall provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.
Addressed by:</td></tr>
</table>

Security Objective	Description
	MOD_UA: FDP_APC_EXT.1/UA, FDP_FIL_EXT.1/UA, FDP_PDC_EXT.1, FDP_PDC_EXT.2/UA, FDP_PDC_EXT.4, FDP_PWR_EXT.1, FDP_SWI_EXT.2
O.NO_USER_DATA_RETENTION	The PSD shall not retain user data in non-volatile memory after power up or, if supported, factory reset. Addressed by: PP_PSD: FDP_RIP_EXT.1
O.NO_OTHER_EXTERNAL_INTERFACES	The PSD shall not have any external interfaces other than those implemented by the TSF. Addressed by: PP_PSD: FDP_PDC_EXT.1
O.LEAK_PREVENTION_SWITCHING	The PSD shall ensure that there are no switching mechanisms that allow signal data leakage between connected computers. Addressed by: PP_PSD: FDP_SWI_EXT.1, FDP_SWI_EXT.2
O.AUTHORIZED_USAGE	The TOE shall explicitly prohibit or ignore unauthorized switching mechanisms, either because it supports only one connected computer or because it allows only authorized mechanisms to switch between connected computers. Authorized switching mechanisms shall require express user action restricted to console buttons, console switches, console touch screen, wired remote control, and peripheral devices using a guard. Unauthorized switching mechanisms include keyboard shortcuts, also known as "hotkeys," automatic port scanning, control through a connected computer, and control through keyboard shortcuts. Where applicable, the results of the switching activity shall be indicated by the TSF so that it is clear to the user that the switching mechanism was engaged as intended. A conformant TOE may also provide a management function to configure some aspects of the TSF. If the TOE provides this functionality, it shall ensure that whatever management functions it provides can only be performed by authorized administrators and that an audit trail of management activities is generated. Addressed by:

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td></td><td><table>
<tr><td>PP_PSD</td><td>FDP_SWI_EXT.1, FDP_SWI_EXT.2, FTA_CIN_EXT.1</td></tr>
<tr><td>MOD_UA</td><td>FDP_FIL_EXT.1/UA</td></tr>
</table></td></tr>
<tr><td>O.PERIPHERAL _PORTS_ISOLATION</td><td>The PSD shall ensure that data does not flow between peripheral devices connected to different PSD interfaces.
Addressed by:<table>
<tr><td>MOD_UA</td><td>FDP_APC_EXT.1/UA, FDP_FIL_EXT.1/UA, FDP_PDC_EXT.1, FDP_PDC_EXT.2/UA, FDP_PDC_EXT.4, FDP_PWR_EXT.1, FDP_SWI_EXT.2</td></tr>
</table></td></tr>
<tr><td>O.REJECT _UNAUTHORIZED _PERIPHERAL</td><td>The PSD shall reject unauthorized peripheral device types and protocols.
Addressed by:<table>
<tr><td>PP_PSD</td><td>FDP_PDC_EXT.1</td></tr>
<tr><td>MOD_UA</td><td>FDP_APC_EXT.1/UA, FDP_FIL_EXT.1/UA, FDP_PDC_EXT.1, FDP_PDC_EXT.2/UA, FDP_PDC_EXT.4, FDP_PWR_EXT.1, FDP_SWI_EXT.2</td></tr>
</table></td></tr>
<tr><td>O.REJECT _UNAUTHORIZED _ENDPOINTS</td><td>The PSD shall reject unauthorized peripheral devices connected via a Universal Serial Bus (USB) hub.
Addressed by:<table>
<tr><td>PP_PSD</td><td>FDP_PDC_EXT.1</td></tr>
<tr><td>MOD_UA</td><td>FDP_APC_EXT.1/UA, FDP_FIL_EXT.1/UA, FDP_PDC_EXT.1, FDP_PDC_EXT.2/UA, FDP_PDC_EXT.4, FDP_PWR_EXT.1, FDP_SWI_EXT.2</td></tr>
</table></td></tr>
<tr><td>O.NO_TOE_ACCESS</td><td>The PSD firmware, software, and memory shall not be accessible via its external ports.
Addressed by:<table>
<tr><td>PP_PSD</td><td>FPT_NTA_EXT.1</td></tr>
</table></td></tr>
<tr><td>O.TAMPER _EVIDENT _LABEL</td><td>The PSD shall be identifiable as authentic by the user and the user must be made aware of any procedures or other such information to accomplish authentication. This feature must be available upon receipt of the PSD and continue to be available during the PSD deployment. The PSD shall be</td></tr>
</table>

Security Objective	Description
	labeled with at least one visible unique identifying tamper-evident marking that can be used to authenticate the device. The PSD manufacturer must maintain a complete list of manufactured PSD articles and their respective identification markings' unique identifiers. Addressed by: PP_PSD: FPT_PHP.1
O.ANTI_TAMPERING	The PSD shall be physically enclosed so that any attempts to open or otherwise access the internals or modify the connections of the PSD would be evident, and optionally thwarted through disablement of the TOE. Note: This applies to a wired remote control as well as the main chassis of the PSD. Addressed by: PP_PSD: FPT_PHP.1
O.SELF_TEST	The PSD shall perform self-tests following power up or powered reset. Addressed by: PP_PSD: FPT_TST.1
O.SELF_TEST _FAIL_TOE _DISABLE	The PSD shall enter a secure state upon detection of a critical failure. Addressed by: PP_PSD: FPT_FLS_EXT.1, FPT_TST_EXT.1
O.SELF_TEST _FAIL_INDICATION	The PSD shall provide clear and visible user indications in the case of a self-test failure. Addressed by: PP_PSD: FPT_TST_EXT.1
O.USER _AUTHENTICATION _ISOLATION	The TOE shall isolate the user authentication function from all other TOE functions. Addressed by: MOD_UA: FDP_UAI_EXT.1

Security Objective	Description
O.SESSION _TERMINATION	The TOE shall immediately terminate an open session with the selected computer upon disconnection of the authentication element. Addressed by: MOD_UA: FDP_TER_EXT.1, FDP_TER_EXT.2, FDP_TER_EXT.3

Table 7 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

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

Security Objective	Description
OE.NO_TEMPEST	The operational environment will not use TEMPEST approved equipment.
OE.PHYSICAL	The operational environment will provide physical security, commensurate with the value of the PSD and the data that transits it.
OE.NO_WIRELESS_DEVICES	The operational environment will not include wireless keyboards, mice, audio, user authentication, or video devices.
OE.TRUSTED_ADMIN	The operational environment will ensure that trusted PSD Administrators and users are appropriately trained.
OE.TRUSTED_CONFIG	The operational environment will ensure that administrators configuring the PSD and its operational environment follow the applicable security configuration guidance.

Table 8 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

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

Threat or Assumption	Security Objective(s)	Rationale
T.DATA_LEAK	O.COMPUTER_INTERFACE_ISOLATION	Isolation of computer interfaces prevents data from leaking between them without authorization.
	O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED	Maintaining interface isolation while the TOE is in an unpowered state ensures that data cannot leak between computer interfaces.
	O.USER_DATA_ISOLATION	The TOE's routing of data only to the selected computer ensures that it will not leak to any others.
	O.NO_OTHER_EXTERNAL_INTERFACES	The absence of additional external interfaces ensures that there is no unexpected method by which data can be leaked.
	O.PERIPHERAL_PORTS_ISOLATION	Isolation of peripheral ports prevents data from leaking between them without authorization.
	O.USER_AUTHENTICATION_ISOLATION	The TOE's user authentication function mitigates this threat by ensuring that the bidirectional channel between the device and the connected computer through the user authentication function is isolated from all other TOE functions.
	O.SESSION_TERMINATION	The TOE mitigates the threat by ensuring that open sessions are terminated and no traffic flows upon disconnection of the authentication element.
T.SIGNAL_LEAK	O.COMPUTER_INTERFACE_ISOLATION	Isolation of computer interfaces prevents data leakage through bit-wise signaling because there is no mechanism by which the signal data can be communicated.
	O.NO_OTHER_EXTERNAL_INTERFACES	The absence of additional external interfaces ensures that there is no unexpected method by which data can be leaked through bitwise signaling.
	O.LEAK_PREVENTION_SWITCHING	The TOE's use of switching methods that are not susceptible to signal leakage helps mitigate the signal leak threat.

Threat or Assumption	Security Objective(s)	Rationale
	O.USER_AUTHENTICATION_ISOLATION	The TOE's user authentication function mitigates this threat by ensuring that the bidirectional channel between the device and the connected computer through the user authentication function is isolated from all other TOE functions.
	O.SESSION_TERMINATION	The TOE mitigates the threat by ensuring that open sessions are terminated and no traffic flows upon disconnection of the authentication element.
T.RESIDUAL_LEAK	O.NO_USER_DATA_RETENTION	The TOE's lack of data retention ensures that a residual data leak is not possible.
	O.USER_AUTHENTICATION_ISOLATION	The TOE's user authentication function mitigates this threat by ensuring that the bidirectional channel between the device and the connected computer through the user authentication function is isolated from all other TOE functions.
	O.SESSION_TERMINATION	The TOE mitigates the threat by ensuring that open sessions are terminated and no traffic flows upon disconnection of the authentication element.
T.UNINTENDED_USE	O.AUTHORIZED_USAGE	The TOE's support for only switching mechanisms that require explicit user action to engage ensures that a user has sufficient information to avoid interacting with an unintended computer.
T.UNAUTHORIZED_DEVICES	O.REJECT_UNAUTHORIZED_ENDPOINTS	The TOE's ability to reject unauthorized endpoints mitigates the threat of unauthorized devices being used to communicate with connected computers.
	O.REJECT_UNAUTHORIZED_PERIPHERAL	The TOE's ability to reject unauthorized peripherals mitigates the threat of unauthorized devices being used to communicate with connected computers.

Threat or Assumption	Security Objective(s)	Rationale
	O.SESSION _TERMINATION	The TOE mitigates the threat by ensuring that open sessions are terminated and no traffic flows upon disconnection of the authentication element.
T.LOGICAL _TAMPER	O.NO_TOE_ACCESS	The TOE's prevention of logical access to its firmware, software, and memory mitigates the threat of logical tampering.
T.PHYSICAL _TAMPER	O.ANTI_TAMPERING	The TOE mitigates the threat of physical tampering through use of an enclosure that provides tamper detection functionality.
	O.TAMPER_EVIDENT _LABEL	The TOE mitigates the threat of physical tampering through use of tamper evident labels that reveal physical tampering attempts.
T.REPLACEMENT	O.TAMPER_EVIDENT _LABEL	The TOE's use of a tamper evident label that provides authenticity of the device mitigates the threat that it is substituted for a replacement device during the acquisition process.
T.FAILED	O.SELF_TEST	The TOE mitigates the threat of failures leading to compromise of security functions through self-tests of its own functionality.
	O.SELF_TEST_FAIL _TOE_DISABLE	The TOE mitigates the threat of failures leading to compromise of security functions by disabling all data flows in the event a failure is detected.
	O.SELF_TEST_FAIL _INDICATION	The TOE mitigates the threat of failures leading to compromise of security functions by providing users with a clear indication when it is in a failure state and should not be trusted.
A.NO_TEMPEST	OE.NO_TEMPEST	If the TOE's operational environment does not include TEMPEST approved equipment, then the assumption is satisfied.

Threat or Assumption	Security Objective(s)	Rationale
A.NO_PHYSICAL	OE.PHYSICAL	If the TOE's operational environment provides physical security, then the assumption is satisfied.
A.NO_WIRELESS _DEVICES	OE.NO_WIRELESS _DEVICES	If the TOE's operational environment does not include wireless peripherals, then the assumption is satisfied.
A.TRUSTED_ADMIN	OE.TRUSTED _ADMIN	If the TOE's operational environment ensures that only trusted administrators will manage the TSF, then the assumption is satisfied.
A.TRUSTED _CONFIG	OE.TRUSTED _CONFIG	If TOE administrators follow the provided security configuration guidance, then the assumption is satisfied.
A.USER_ALLOWED _ACCESS	OE.PHYSICAL	If the TOE's operational environment provides physical access to connected computers, then the assumption is satisfied.

Table 9 – Security Objectives Rationale

5 EXTENDED COMPONENTS DEFINITION

The extended components definition is presented in Appendix C of the Protection Profile for Peripheral Sharing Device [PP_PSD_V4.0] and in the module for user authentication devices [MOD_UA_V1.0]. It is repeated here to ensure the completeness of this ST.

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

Functional Class	Functional Families
User Data Protection (FDP)	FDP_APC_EXT Active PSD Connections
	FDP_FIL_EXT Device Filtering
	FDP_PDC_EXT Peripheral Device Connection
	FDP_PWR_EXT Powered By Computer
	FDP_RIP_EXT Residual Information Protection
	FDP_SWI_EXT PSD Switching
	FDP_TER_EXT Session Termination
	FDP_UAI_EXT User Authentication Isolation
Protection of the TSF (FPT)	FPT_FLS_EXT Failure with Preservation of Secure State
	FPT_NTA_EXT No Access to TOE
	FPT_TST_EXT TSF Testing
TOE Access (FTA)	FTA_CIN_EXT Continuous Indications

Table 10 – Functional Families of Extended Components

5.1 CLASS FDP: USER DATA PROTECTION

5.1.1 FDP_APC_EXT Active PSD Connections

Family Behavior

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

Component Leveling

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

Management: FDP_APC_EXT.1

No specific management functions are identified.

Audit: FDP_APC_EXT.1

There are no auditable events foreseen.

FDP_APC_EXT.1 Active PSD Connections

Hierarchical to:	No other components.
Dependencies:	No dependencies
FDP_APC_EXT.1.1	The TSF shall route user data only to or from the interfaces selected by the user.
FDP_APC_EXT.1.2	The TSF shall ensure that no data flows between connected computers whether the TOE is powered on or powered off.
FDP_APC_EXT.1.3	The TSF shall ensure that no data transits the TOE when the TOE is powered off.
FDP_APC_EXT.1.4	The TSF shall ensure that no data transits the TOE when the TOE is in a failure state.

5.1.2 FDP_FIL_EXT Device Filtering

Family Behavior

Components in this family define the requirements for device filtering.

Component Leveling

FDP_FIL_EXT.1 Device Filtering, requires the TSF to specify the method of device filtering used for peripheral interfaces and defines requirements for handling whitelists and blacklists.

Management: FDP_FIL_EXT.1

The following actions could be considered for the management functions in FMT:

- Ability to configure whitelist/blacklist members

Audit: FDP_FIL_EXT.1

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Configuration of whitelist/blacklist members

FDP_FIL_EXT.1 Device Filtering

Hierarchical to:	No other components
Dependencies:	FDP_PDC_EXT.1 Peripheral Device Connection
FDP_FIL_EXT.1.1	The TSF shall have [*selection: configurable, fixed*] device filtering for [*assignment: list of supported peripheral interface types*] interfaces.
FDP_FIL_EXT.1.2	The TSF shall consider all [*assignment: blacklist name*] blacklisted devices as unauthorized devices for [*assignment: list of supported peripheral interface types*] interfaces in peripheral device connections.
FDP_FIL_EXT.1.3	The TSF shall consider all [*assignment: whitelist name*] whitelisted devices as authorized devices for peripheral device connections only if they are not on the [*assignment: blacklist name*] blacklist or otherwise unauthorized.

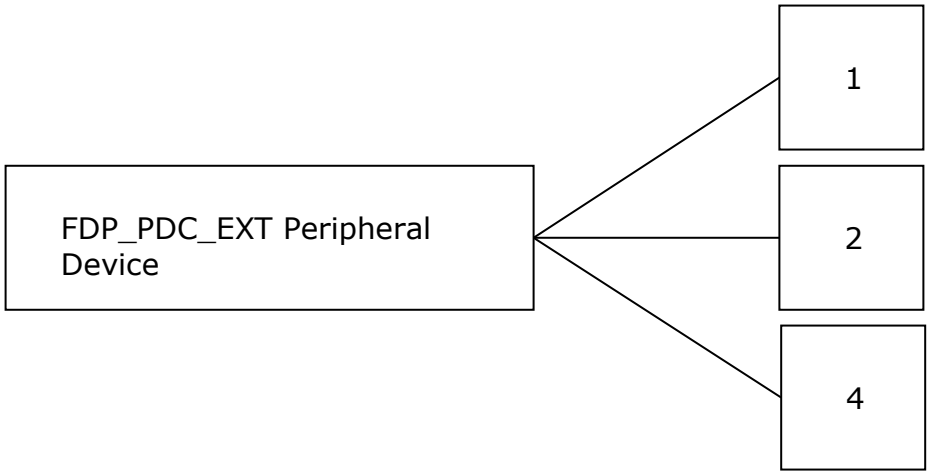
5.1.3 FDP_PDC_EXT Peripheral Device Connection

Family Behavior

Components in this family define the requirements for peripheral device connections.

This family is defined in the PSD PP. This PP-Module [MOD_UA_V1.0] augments the extended family by adding two additional components, FDP_PDC_EXT.2 and FDP_PDC_EXT.4. The new components and their impact on the extended family's component leveling are shown below; reference the PSD PP for all other definitions for this family.

Component Leveling



FDP_PDC_EXT.1 Peripheral Device Connection, requires the TSF to limit external connections to only authorized devices.

FDP_PDC_EXT.2 Authorized Devices, defines the types of physical devices that the TSF will permit to connect to it.

FDP_PDC_EXT.4 Supported Authentication Devices, defines whether the TSF includes an internal or external authentication device.

Management: FDP_PDC_EXT.1, FDP_PDC_EXT.2, FDP_PDC_EXT.4

No specific management functions are identified.

Audit: FDP_PDC_EXT.1

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Acceptance or rejection of a peripheral

Audit: FDP_PDC_EXT.2, FDP_PDC_EXT.4

There are no specific auditable events foreseen.

FDP_PDC_EXT.1 Peripheral Device Connection

Hierarchical to:	No other components.
Dependencies:	No dependencies
FDP_PDC_EXT.1.1	The TSF shall reject connections with unauthorized devices upon TOE power up and upon connection of a peripheral device to a powered-on TOE.
FDP_PDC_EXT.1.2	The TSF shall reject connections with devices presenting unauthorized interface protocols upon TOE power up and upon connection of a peripheral device to a powered-on TOE.
FDP_PDC_EXT.1.3	The TOE shall have no external interfaces other than those claimed by the TSF.
FDP_PDC_EXT.1.4	The TOE shall not have wireless interfaces.

FDP_PDC_EXT.1.5 The TOE shall provide a visual or auditory indication to the User when a peripheral is rejected.

FDP_PDC_EXT.2 Authorized Devices

Hierarchical to: No other components.

Dependencies: FDP_PDC_EXT.1 Peripheral Device Connection

FDP_PDC_EXT.2.1 The TSF shall allow connections with authorized devices as defined in [*assignment: devices specified in the PP or PP-Module in which this SFR is defined*] and [*assignment: devices specified in another PP or PP-Module that shares a PP Configuration with the PP or PP-Module in which this SFR is defined*] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.2.2 The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in [*assignment: devices specified in the PP or PP Module in which this SFR is defined*] and [*assignment: devices specified in another PP or PP-Module that shares a PP-Configuration with the PP or PP-Module in which this SFR is defined*] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.4 Supported Authentication Devices

Hierarchical to: No other components.

Dependencies: FDP_PDC_EXT.1 Peripheral Device Connection,
FDP_PDC_EXT.2 Authorized Devices

FDP_PDC_EXT.4.1 The TSF shall have an [selection: internal, external] user authentication device.

5.1.4 FDP_PWR_EXT Powered By Computer

Family Behavior

Components in this family define the requirements for device powering.

Component Leveling

FDP_PWR_EXT.1 Powered by Computer, requires the TSF to not be powered by a connected computer.

Management: FDP_PWR_EXT.1

No specific management functions are identified.

Audit: FDP_PWR_EXT.1

There are no specific auditable events foreseen.

FDP_PWR_EXT.1 Powered By Computer

Hierarchical to: No other components.

Dependencies: No dependencies

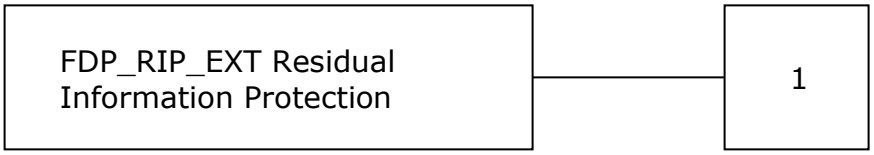
FDP_PWR_EXT.1.1 The TSF shall not be powered by a connected computer.

5.1.5 FDP_RIP_EXT Residual Information Protection

Family Behavior

Components in this family define the requirements for how the TSF prevents data disclosure from its memory.

Component Leveling



FDP_RIP_EXT.1 Residual Information Protection, requires the TSF to prevent the writing of user data to non-volatile memory.

Management: FDP_RIP_EXT.1

The following actions could be considered for the management functions in FMT:

- Ability to trigger the TSF's purge function

Audit: FDP_RIP_EXT.1

There are no auditable events foreseen.

FDP_RIP_EXT.1 Residual Information Protection

Hierarchical to: No other components.

Dependencies: No dependencies

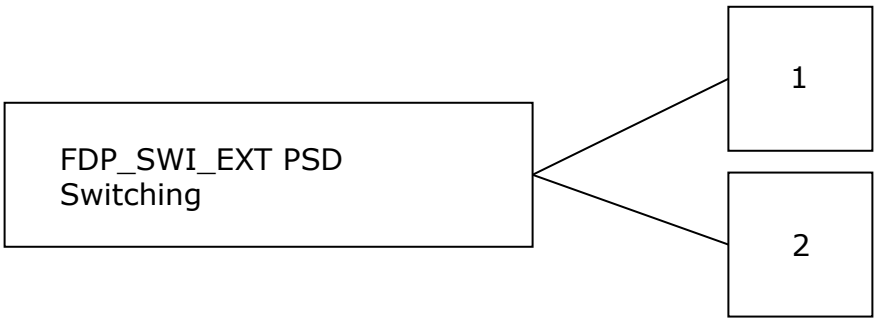
FDP_RIP_EXT.1.1 The TSF shall ensure that no user data is written to TOE non-volatile memory or storage.

5.1.6 FDP_SWI_EXT PSD Switching

Family Behavior

Components in this family define the requirements for how the TSF protects against inadvertent data switching.

Component Leveling



FDP_SWI_EXT.1 PSD Switching, requires action on the part of a user in order for the TSF's switching mechanisms to be activated.

FDP_SWI_EXT.2 PSD Switching Methods, places restrictions on how the TSF's switching mechanisms can be controlled.

Management: FDP_SWI_EXT.1, FDP_SWI_EXT.2

No specific management functions are identified.

Audit: FDP_SWI_EXT.1, FDP_SWI_EXT.2

There are no auditable events foreseen.

FDP_SWI_EXT.1 PSD Switching

Hierarchical to: No other components.

Dependencies: No dependencies

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

FDP_SWI_EXT.2 PSD Switching Methods

Hierarchical to: No other components.

Dependencies: FDP_SWI_EXT.1 PSD Switching

FDP_SWI_EXT.2.1 The TSF shall ensure that no switching can be initiated through automatic port scanning, control through a connected computer, or control through keyboard shortcuts.

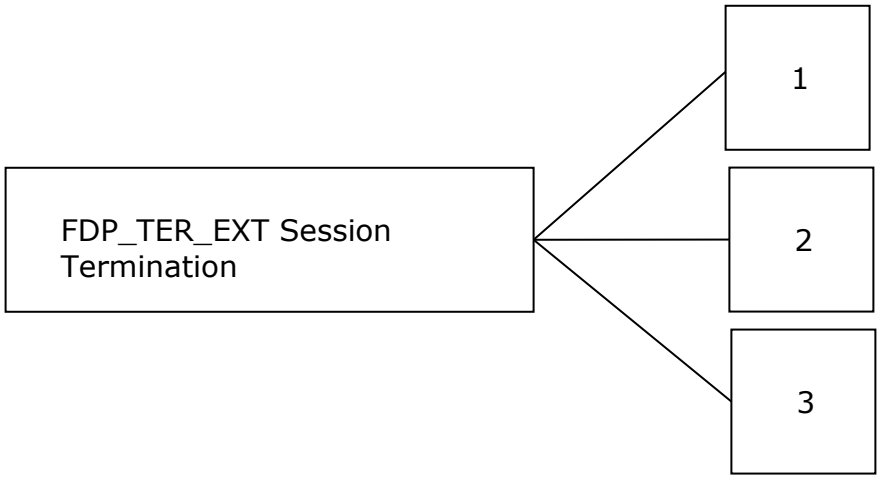
FDP_SWI_EXT.2.2 The TSF shall ensure that switching can be initiated only through express user action using [*selection: console buttons, console switches, console touch screen, wired remote control, peripheral devices using a guard*].

5.1.7 FDP_TER_EXT Session Termination

Family Behavior

Components in this family define the requirements for termination of open sessions.

Component Leveling



FDP_TER_EXT.1, Session Termination, requires the TSF to terminate an open session upon removal of the authentication element.

FDP_TER_EXT.2, Session Termination of Removed Devices, requires the TSF to terminate an open session upon removal of the user authentication device.

FDP_TER_EXT.3, Session Termination upon Switching, requires the TOE to terminate an open session upon switching to a different computer; and reset the power to the user authentication device for at least one second upon switching to a different computer.

Management: FDP_TER_EXT.1, FDP_TER_EXT.2, FDP_TER_EXT.3

No specific management functions are identified.

Audit: FDP_TER_EXT.1, FDP_TER_EXT.2, FDP_TER_EXT.3

There are no specific auditable events foreseen.

FDP_TER_EXT.1 Session Termination

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_TER_EXT.1.1 The TSF shall terminate an open session upon removal of the authentication element.

FDP_TER_EXT.2 Session Termination of Removed Devices

Hierarchical to: No other components.

Dependencies: FDP_PDC_EXT.2 Authorized Devices

FDP_TER_EXT.2.1 The TSF shall terminate an open session upon removal of the user authentication device.

FDP_TER_EXT.3 Session Termination upon Switching

Hierarchical to: No other components.

Dependencies: FDP_SWI_EXT.1 PSD Switching

FDP_TER_EXT.3.1 The TSF shall terminate an open session upon switching to a different computer.

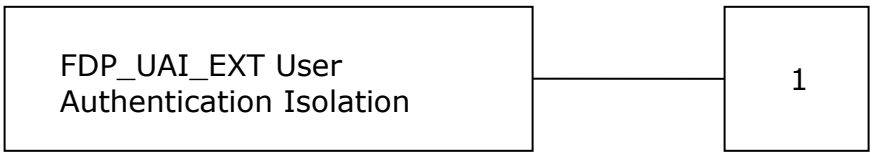
FDP_TER_EXT.3.2 The TSF shall reset the power to the user authentication device for at least one second upon switching to a different computer.

5.1.8 FDP_UAI_EXT User Authentication Isolation

Family Behavior

Components in this family define the requirements for user authentication isolation.

Component Leveling



FDP_UAI_EXT.1 User Authentication Isolation, requires the TSF to isolate the user authentication function from all other TOE USB functions.

Management: FDP_UAI_EXT.1

No specific management functions are identified.

Audit: FDP_UAI_EXT.1

There are no specific auditable events foreseen.

FDP_UAI_EXT.1 User Authentication Isolation

Hierarchical to: No other components.

Dependencies: None

FDP_UAI_EXT.1.1 The TSF shall isolate the user authentication function from all other TOE USB functions.

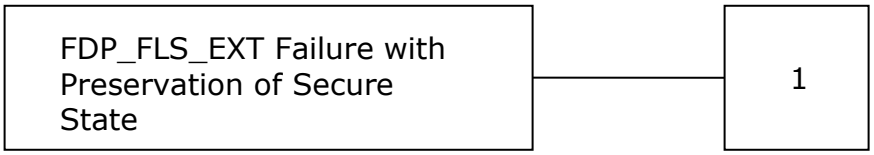
5.2 CLASS FPT: PROTECTION OF THE TSF

5.2.1 FPT_FLS_EXT Failure with Preservation of Secure State

Family Behavior

Components in this family define the secure failure requirements for the TSF.

Component Leveling



FPT_FLS_EXT.1 Failure with Preservation of Secure State, requires the TSF to go into a secure state upon the detection of selected failures.

Management: FPT_FLS_EXT.1

No specific management functions are identified.

Audit: FPT_FLS_EXT.1

There are no auditable events foreseen.

FPT_FLS_EXT.1 Failure with Preservation of Secure State

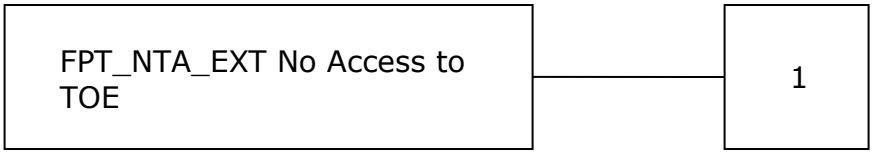
Hierarchical to:	No other components.
Dependencies:	FPT_TST.1 TSF Testing FPT_PHP.3 Resistance to Physical Attack
FPT_FLS_EXT.1.1	The TSF shall preserve a secure state when the following types of failures occur: failure of the power-on self-test and [*selection: failure of the anti-tamper function, no other failures*].

5.2.2 FPT_NTA_EXT No Access to TOE

Family Behavior

Components in this family define what TSF information may be externally accessible.

Component Leveling



FPT_NTA_EXT.1 No Access to TOE, requires the TSF to block access to non-authorized TSF data via external ports.

Management: FPT_NTA_EXT.1

No specific management functions are identified.

Audit: FPT_NTA_EXT.1

There are no auditable events foreseen.

FPT_NTA_EXT.1 No Access to TOE

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_NTA_EXT.1.1 TOE firmware, software, and memory shall not be accessible via the TOE's external ports, with the following exceptions: [*selection: the EDID memory of Video TOEs may be accessible from connected computers; the configuration data, settings, and logging data that may be accessible by authorized administrators; no other exceptions*].

5.2.3 FPT_TST_EXT TSF Testing

Family Behavior

Components in this family define how the TSF responds to a self-test failure.

Component Leveling

FPT_TST_EXT.1 TSF Testing, requires the TSF to shutdown normal functions and provide a visual or auditory indication that a self-test has failed.

Management: FPT_TST_EXT.1

No specific management functions are identified.

Audit: FPT_TST_EXT.1

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Indication that the TSF self-test was completed
- Failure of self-test

FPT_TST_EXT.1 TSF Testing

Hierarchical to: No other components.

Dependencies: FPT_TST.1 TSF Testing

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

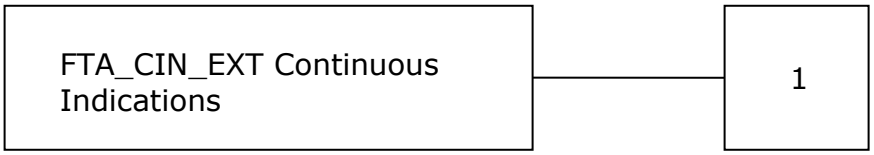
5.3 CLASS FTA: TOE ACCESS

5.3.1 FTA_CIN_EXT Continuous Indications

Family Behavior

Components in this family define how the TSF displays its switching status.

Component Leveling



FTA_CIN_EXT.1 Continuous Indications, requires the TSF to display a visual indication of what computers are selected.

Management: FTA_CIN_EXT.1

No specific management functions are identified.

Audit: FTA_CIN_EXT.1

There are no auditable events foreseen.

FTA_CIN_EXT.1 Continuous Indications

Hierarchical to:	No other components.
Dependencies:	FDP_APC_EXT.1 Active PSD Connections
FTA_CIN_EXT.1.1	The TSF shall display a visible indication of the selected computers at all times when the TOE is powered.
FTA_CIN_EXT.1.2	The TSF shall implement the visible indication using the following mechanism: **easily visible graphical and/or textual markings of each source video on the display,** [*selection: a button, a panel with lights, a screen with dimming function, a screen with no dimming function, [assignment: description of visible indication]*].
FTA_CIN_EXT.1.3	The TSF shall ensure that while the TOE is powered the current switching status is reflected by [*selection: the indicator, multiple indicators which never display conflicting information*].

6 SECURITY REQUIREMENTS

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

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations are shown using the same conventions as those in the PSD PP. This is defined in the PP as:

- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*].
- Selection: Indicated by surrounding brackets and italics, e.g., [*selected item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Iteration operations are identified with a slash ('/') and an identifier (e.g. "/UA").

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

6.2 SECURITY FUNCTIONAL REQUIREMENTS

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

Class	Identifier	Name
User Data Protection (FDP)	FDP_APC_EXT.1/UA	Active PSD Connections
	FDP_FIL_EXT.1/UA	Device Filtering (User Authentication Devices)
	FDP_PDC_EXT.1	Peripheral Device Connection
	FDP_PDC_EXT.2/UA	Authorized Devices (User Authentication Devices)
	FDP_PDC_EXT.4	Supported Authentication Device
	FDP_PWR_EXT.1	Powered By Computer
	FDP_RIP_EXT.1	Residual Information Protection
	FDP_SWI_EXT.1	PSD Switching
	FDP_SWI_EXT.2	PSD Switching Methods

Class	Identifier	Name
	FDP_TER_EXT.1	Session Termination
	FDP_TER_EXT.2	Session Termination of Removed Devices
	FDP_TER_EXT.3	Session Termination upon Switching
	FDP_UAI_EXT.1	User Authentication Isolation
Protection of the TSF (FPT)	FPT_FLS_EXT.1	Failure with Preservation of Secure State
	FPT_NTA_EXT.1	No Access to TOE
	FPT_PHP.1	Passive Detection of Physical Attack
	FPT_TST.1	TSF testing
	FPT_TST_EXT.1	TSF Testing
TOE Access (FTA)	FTA_CIN_EXT.1	Continuous Indications

Table 11 – Summary of Security Functional Requirements

6.2.1 User Data Protection (FDP)

6.2.1.1 FDP_APC_EXT.1/UA Active PSD Connections

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

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

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

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

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

FDP_FIL_EXT.1.1/UA The TSF shall have [*fixed*] device filtering for [*user authentication device*] interfaces.

FDP_FIL_EXT.1.2/UA The TSF shall consider all [*PSD UA*] blacklisted devices as unauthorized devices for [*user authentication device*] interfaces in peripheral device connections.

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

6.2.1.3 FDP_PDC_EXT.1 Peripheral Device Connection

FDP_PDC_EXT.1.1 The TSF shall reject connections with unauthorized devices upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.1.2 The TSF shall reject connections with devices presenting unauthorized interface protocols upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.1.3 The TOE shall have no external interfaces other than those claimed by the TSF.

FDP_PDC_EXT.1.4 The TOE shall not have wireless interfaces.

FDP_PDC_EXT.1.5 The TOE shall provide a visual or auditory indication to the User when a peripheral is rejected.

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

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

- ***no other devices***

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

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

- ***no other devices***

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

6.2.1.5 FDP_PDC_EXT.4 Supported Authentication Device

FDP_PDC_EXT.4.1 The TSF shall have an [*internal*] user authentication device.

6.2.1.6 FDP_PWR_EXT.1 Powered By Computer

FDP_PWR_EXT.1.1 The TSF shall not be powered by a connected computer.

6.2.1.7 FDP_RIP_EXT.1 Residual Information Protection

FDP_RIP_EXT.1.1 The TSF shall ensure that no user data is written to TOE non-volatile memory or storage.

6.2.1.8 FDP_SWI_EXT.1 PSD Switching

FDP_SWI_EXT.1.1 The TSF shall ensure that [*switching can be initiated only through express user action*].

6.2.1.9 FDP_SWI_EXT.2 PSD Switching Methods

FDP_SWI_EXT.2.1 The TSF shall ensure that no switching can be initiated through automatic port scanning, control through a connected computer, or control through keyboard shortcuts.

FDP_SWI_EXT.2.2 The TSF shall ensure that switching can be initiated only through express user action using [*console buttons*].

6.2.1.10 FDP_TER_EXT.1 Session Termination

FDP_TER_EXT.1.1 The TSF shall terminate an open session upon removal of the authentication element.

6.2.1.11 FDP_TER_EXT.2 Session Termination of Removed Devices

FDP_TER_EXT.2.1 The TSF shall terminate an open session upon removal of the user authentication device.

6.2.1.12 FDP_TER_EXT.3 Session Termination upon Switching

FDP_TER_EXT.3.1 The TSF shall terminate an open session upon switching to a different computer.

FDP_TER_EXT.3.2 The TSF shall reset the power to the user authentication device for at least one second upon switching to a different computer.

6.2.1.13 FDP_UAI_EXT.1 User Authentication Isolation

FDP_UAI_EXT.1.1 The TSF shall isolate the user authentication function from all other TOE USB functions.

6.2.2 Protection of the TSF (FPT)

6.2.2.1 FPT_FLS_EXT.1 Failure with Preservation of Secure State

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

6.2.2.2 FPT_NTA_EXT.1 No Access to TOE

FPT_NTA_EXT.1.1 TOE firmware, software, and memory shall not be accessible via the TOE's external ports, with the following exceptions: [*no other exceptions*].

6.2.2.3 FPT_PHP.1 Passive Detection of Physical Attack

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

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

6.2.2.4 FPT_TST.1 TSF Testing

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

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

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

6.2.2.5 FPT_TST_EXT.1 TSF Testing

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

6.2.3 TOE Access (FTA)

6.2.3.1 FTA_CIN_EXT.1 Continuous Indications

FTA_CIN_EXT.1.1 The TSF shall display a visible indication of the selected computers at all times when the TOE is powered.

FTA_CIN_EXT.1.2 The TSF shall implement the visible indication using the following mechanism: [*a panel with lights*].

FTA_CIN_EXT.1.3 The TSF shall ensure that while the TOE is powered the current switching status is reflected by [*the indicator*].

6.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 12.

Assurance Class	Assurance Components	
	Identifier	**Name**
Development (ADV)	ADV_FSP.1	Basic Functional Specification
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support (ALC)	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM[2] Coverage
Security Target Evaluation (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Tests (ATE)	ATE_IND.1	Independent Testing - Conformance
Vulnerability Assessment (AVA)	AVA_VAN.1	Vulnerability Survey

Table 12 – Security Assurance Requirements

6.4 SECURITY REQUIREMENTS RATIONALE

6.4.1 Security Functional Requirements Rationale

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

[2] Configuration Management

6.4.2 Dependency Rationale

Table 13 identifies the Security Functional Requirements and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependencies	Rationale Statement
FDP_APC_EXT.1/UA	None	N/A
FDP_FIL_EXT.1/UA	FDP_PDC_EXT.1	Included
FDP_PDC_EXT.1	None	N/A
FDP_PDC_EXT.2/UA	FDP_PDC_EXT.1	Included
FDP_PDC_EXT.4	FDP_PDC_EXT.1 FDP_PDC_EXT.2	Included
FDP_PWR_EXT.1	None	N/A
FDP_RIP_EXT.1	None	N/A
FDP_SWI_EXT.1	None	N/A
FDP_SWI_EXT.2	FDP_SWI_EXT.1	Included
FDP_TER_EXT.1	None	N/A
FDP_TER_EXT.2	FDP_PDC_EXT.2	Included
FDP_TER_EXT.3	FDP_SWI_EXT.1	Included
FDP_UAI_EXT.1	None	N/A
FPT_FLS_EXT.1	FPT_TST.1 FPT_PHP.3	Included Included only if anti-tamper is selected in FPT_FLS_EXT.1.1
FPT_NTA_EXT.1	None	N/A
FPT_PHP.1	None	N/A
FPT_TST.1	None	N/A
FPT_TST_EXT.1	FPT_TST.1	Included
FTA_CIN_EXT.1	FDP_APC_EXT.1	Included

Table 13 – Functional Requirement Dependencies

6.4.3 Security Assurance Requirements Rationale

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

7 TOE SUMMARY SPECIFICATION

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

7.1 USER DATA PROTECTION

7.1.1 System Controller

The device includes a System Controller which is responsible for device management, user interaction, system control security functions, and device monitoring. It receives user input from the switches on the front panel, and drives the TOE channel select lines that control switching circuits within the TOE.

The System Controller includes a microcontroller with internal non-volatile, Read Only Memory (ROM). The controller function manages the TOE functionality through a pre-programmed state machine loaded on the ROM as read-only firmware during product manufacturing.

Following boot up of the Multi-Domain Smart Card Reader, the channel select lines are set to Channel 1 by default. The user determines the host computer to be connected to the peripherals by pressing a button on the TOE front panel. The Light Emitting Diode (LED) above the front panel button of the selected computer is illuminated. Switching can only be initiated through express user action.

TOE Security Functional Requirements addressed: FDP_SWI_EXT.1, FDP_SWI_EXT.2.

7.1.1.1 Active PSD Connections

The TOE ensures that data flows only between the card reader and the connected computer selected by the user. No data transits the TOE when the TOE is powered off, or when the TOE is in a failure state. A failure state occurs when the TOE fails a self-test when powering on.

TOE Security Functional Requirements addressed: FDP_APC_EXT.1/UA.

7.1.1.2 Connected Computer Interfaces

The Multi-Domain Smart Card Reader includes a card reader and cables which are attached to the connected computers. The TOE presents a USB type A cable interface to be attached to each connected computer.

TOE Security Functional Requirements addressed: FDP_PDC_EXT.1.

7.1.1.3 Residual Information Protection

The Letter of Volatility is included as Annex A.

TOE Security Functional Requirements addressed: FDP_RIP_EXT.1.

7.1.2 Smart Card Reader Switching Functionality

The Multi-Domain Smart Card Reader device is a secure card reader that allows a single user smartcard to authenticate with up to four isolated computers.

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.

Computer interfaces are isolated. Each computer interface uses independent circuitry and power planes. There is no shared circuitry, and no shared logical functions.

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.

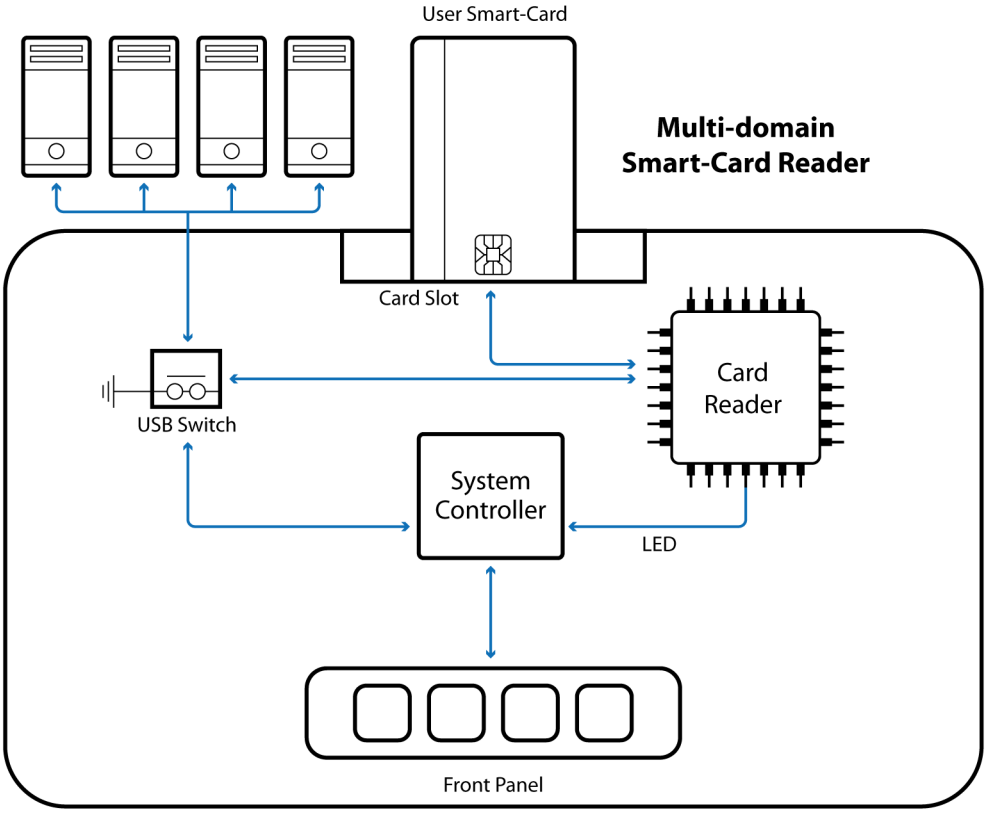


Figure 2 – Multi-Domain Smart Card Reader

Following a failed self-test, or when the TOE is powered off, all user authentication device data paths are isolated through a peripheral multiplexer. These events effectively disconnect any open authentication session. Removal of the authentication device will also close the authentication session.

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.

TOE Security Functional Requirements addressed: FDP_FIL_EXT.1/UA, FDP_PWR_EXT.1, FDP_TER_EXT.1, FDP_TER_EXT.2, FDP_TER_EXT.3, FDP_UAI_EXT.1.

7.1.2.1 User Authentication Compatible Device Types

The Vertiv Multi-Domain Smart Card Reader includes an internal authentication device. The TOE's USB cables are plugged into the connected computers. The TOE does not support wireless connections of any type.

TOE Security Functional Requirements addressed: FDP_PDC_EXT.1, FDP_PDC_EXT.2/UA, FDP_PDC_EXT.4.

7.2 PROTECTION OF THE TSF

7.2.1 No Access to TOE

Connected computers do not have access to TOE firmware or memory.

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

TOE Security Functional Requirements addressed: FPT_NTA_EXT.1.

7.2.2 Passive Anti-tampering Functionality

The TOE enclosure was designed specifically to prevent physical tampering. It features molded plastic parts connected by screws. Each device is fitted with a 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.

TOE Security Functional Requirements addressed: FPT_PHP.1.

7.2.3 TSF Testing

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

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

If the self-test fails, the LEDs on the front panel blink and the device makes a beeping 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.

TOE Security Functional Requirements addressed: FPT_FLS_EXT.1, FPT_TST.1, FPT_TST_EXT.1.

7.3 TOE ACCESS

The TOE user switches between computers by pressing the corresponding front panel button on the device. The LED above the front panel button corresponding to the selected computer will illuminate.

Figure 1 shows the selection buttons.

On power up and the successful completion of the self-test, or power up following reset and the successful completion of the self-test, the smartcard is 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.

TOE Security Functional Requirements addressed: FTA_CIN_EXT.1.

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
Authentication element	The term 'authentication element' is used in [MOD_UA_V1.0] to describe the physical object used to identify the user. This could be a smart card, proximity card or, in the case of a biometric authentication device, a user's hand. For this TOE, it refers to a smart card.
UA	UA refers to the requirements for User Authentication Devices.
User Authentication Device	The term 'User Authentication Device' is defined in [MOD_UA_V1.0] as, "A peripheral device used to authenticate the identity of the user, such as a smartcard reader, biometric authentication device, or proximity card reader."

Table 14 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
CAC	Common Access Card
CC	Common Criteria
CCID	Chip Card Interface Device
CM	Configuration Management
EEPROM	Electrically Erasable Programmable Read-Only Memory
FET	Field Effect Transistor
IT	Information Technology
JTAG	Joint Test Action Group
LED	Light Emitting Diode
MCU	Microcontroller unit
MDR	Multi-Domain Car Reader (or Multi-Domain Reader)
NIAP	National Information Assurance Partnership
OTP	One Time Programming

Acronym	Definition
PP	Protection Profile
PSD	Peripheral Sharing Device
ROM	Read Only Memory
SFR	Security Functional Requirement
SRAM	Static Random Access Memory
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
USB	Universal Serial Bus

Table 15 – Acronyms

9 REFERENCES

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017 • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017 • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1 Revision 5, April 2017
[PP_PSD_V4.0]	Protection Profile for Peripheral Sharing Device, Version: 4.0, 2019-07-19
[MOD_UA_V1.0]	PP-Module for User Authentication Devices, Version 1.0, 2019-07-19
[CFG_PSD-UA_V1.0]	PP-Configuration for Peripheral Sharing Device and User Authentication Devices, 19 July 2019

Table 16 – References

ANNEX A – LETTER OF VOLATILITY

The table below provides volatility information and memory types for the Vertiv Multi-Domain Smart Card Reader. User data is not retained in any TOE device when the power is turned off.

Product Model	Number in each product	Function, Manufacturer and Part Number	Storage Type	Size	Power Source (if not the TOE)	Volatility	Contains User Data
SCMDR0001	1	System Controller: ST Microelectronics STM32F446ZCT	Embedded SRAM	128KB		Volatile	May contain user data
			Embedded Flash[1]	256KB		Non-Volatile	No user data
			Embedded EEPROM	4KB		Non-Volatile	No user data
			OTP Memory	512bytes		Non-Volatile	No user data
	1	Card Reader: Alcor Micro AU9540	Smart Card Control RAM	256bytes		Volatile	May contain user data
			Embedded EEPROM	8KB		Non-Volatile	No user data
			Optional EEPROM[2]	256bytes		Non-Volatile	No user data

Notes:

[1] Flash storage is used to store firmware code. It contains no user data. Flash storage is permanently locked by fuses after initial programming to prevent rewriting. It is an integral part of the ST Microcontroller together with SRAM and EEPROM.

[2] The component includes an externally accessible EEPROM for the purpose of storing the VID and PID. This is not used in the TOE. This EEPROM is inaccessible once implemented in the TOE.