I/O INTERCONNECT

I O INTERCONNECT Secure KVM Security Target

Document ID

Version: 1.2

May 10, 2018

Prepared For:

I O INTERCONNECT LTD

1202 E Wakeham Ave.
Santa Ana, CA 92705

Prepared By:

UL Verification Services Inc.

Notices:

1 Introduction

- The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.
- The ST reference shall uniquely identify the ST.
- The TOE reference shall identify the TOE.

The structure of this document is defined by CC v3.1r4 Part 1 Annex A.2, “Mandatory contents of an ST”:

- Section 1 contains the ST Introduction, including the ST reference, Target of Evaluation (TOE) reference, TOE overview, and TOE description.
- Section 2 contains conformance claims to the Common Criteria (CC) version, Protection Profile (PP) and package claims, as well as rationale for these conformance claims.
- Section 3 contains the security problem definition, which includes threats, Organizational Security Policies (OSP), and assumptions that must be countered, enforced, and upheld by the TOE and its operational environment.
- Section 4 contains statements of security objectives for the TOE, and the TOE operational environment as well as rationale for these security objectives.
- Section 5 contains definitions of any extended security requirements claimed in the ST.
- Section 6 contains the security function requirements (SFR), the security assurance requirements (SAR), as well as the rationale for the claimed SFR and SAR.
- Section 7 contains the TOE summary specification, which includes the detailed specification of the IT security functions

1.1 Security Target Reference

The Security Target reference shall uniquely identify the Security Target.

ST Title:	I O INTERCONNECT Secure KVM Security Target
ST Version:	1.2
ST Author(s):	Kenji Yoshino, Brad Mitchell
ST Publication Date:	May 10, 2018
Keywords	Peripheral Sharing Switch

1.2 Target of Evaluation Reference

The Target of Evaluation reference shall identify the Target of Evaluation (TOE).

TOE Developer	I O INTERCONNECT LTD
	1202 E Wakeham Ave.
	Santa Ana, CA 92705
TOE Name:	Secure KVM
TOE Version:	1.0

1.3 PP Identification

Protection Profile for Peripheral Sharing Switch (PSS), Version 3.0, 13 February 2015

1.4 TOE Overview

1.4.1 TOE Product Type

The TOE is classified as a Peripheral Sharing Switch.

1.4.2 TOE Usage

The TOE allows a user to use a single set of peripherals (Keyboard, Mouse, CAC Reader, Speakers, and/or video devices) with multiple computers. The TOE allows the user to easily switch which computer the peripherals are connected to by pressing a button on the TOE. The TOE ensures the peripherals are only connected to a single computer at a time and prevents the computers from communicating with each other through the TOE. The TOE consists of a stand-alone KVM (Keyboard, Video, Mouse) switching unit or a KVM with a Desktop Control Unit (DCU). The DCU is a small device that provides channel switching buttons and selection channel indicators allowing the user to save even more desk space.

1.4.3 TOE Major Security Features Summary

- User Data Protection and Data Isolation
- Protection of the TSF
- TOE Access

1.4.4 TOE IT environment hardware/software/firmware requirements

The TOE requires an environment that provides steady power and satisfies the requirements specified in Section 4.2.

The following peripheral devices from the operational environment may be connected to the TOE in the evaluated configuration:

- PS/2 Keyboard
- PS/2 Mouse
- USB Mouse
- USB Keyboard
- USB CAC Reader
- Analog Audio Speakers or Headphones
- Video device(s) supporting DVI-D, DisplayPort v1.2a, or HDMI v1.4. See the Peripheral Video Interface column in Table 1 to determine which interfaces are compatible with each model of the TOE.

The following computer interfaces from the operational environment may be connected to the TOE in the evaluated configuration:

- USB 2.0 (for Mouse and Keyboard Input)
- USB 2.0 (for CAC input)

- Analog Audio Out
- Video output supporting DVI, DisplayPort, or HDMI. See the Computer Video Interface column in Table 1 to determine which interfaces are compatible with each model of the TOE.

The TOE will switch all compatible and authorized devices attached; however, it does not require all peripheral or computer interfaces to be populated.

1.5 TOE Description

1.5.1 TOE Physical Boundaries

The TOE physical boundary consists of the hardware and firmware identified below:

- KVM Hardware:
    - SV141D1
    - SV141D0
    - SV241D1
    - SV241D0
    - SV121D1
    - SV121D0
    - SV142H1
    - SV142H0
    - SV242H1
    - SV242H0
    - SV142P1
    - SV142P0
    - SV122P1
    - SV122P0
    - SV242P1
    - SV242P0
    - SV222P1
    - SV222P0
- KVM Firmware:
    - Firmware Version 26B-29B
- DCU Hardware:
    - AR000010
- DCU Firmware:
    - Firmware Version 288

The guidance documentation that is part of the TOE is listed in Section 9 “References” within Table 11: TOE Guidance Documentation. The TOE also consists of the evaluation evidence listed in Section 9 “References” Table 12: TOE Evaluation Evidence.

The TOE consists of one of the KVM hardware models and KVM hardware models with the DCU hardware.

The hardware models contain the following capabilities:

Table 1: TOE Models

Model	Computer Port Groups	Display Channels	Computer Video Interface	Peripheral Video Interface	CAC	Description
SV141D1	4	Single	Dual Link DVI-D	Dual Link DVI-D	Y	4 Port Single DVI 4K video Secure KVM with CAC PP3.0
SV141D0	4	Single	Dual Link DVI-D	Dual Link DVI-D	N	4 Port Single DVI 4K video Secure KVM without CAC PP3.0
SV241D1	4	Dual	Dual Link DVI-D	Dual Link DVI-D	Y	4 Port Dual DVI 4K video Secure KVM with CAC PP3.0
SV241D0	4	Dual	Dual Link DVI-D	Dual Link DVI-D	N	4 Port Dual DVI 4K video Secure KVM without CAC PP3.0
SV121D1	2	Single	Dual Link DVI-D	Dual Link DVI-D	Y	2 port Single DVI 4K video Secure KVM with CAC PP3.0
SV121D0	2	Single	Dual Link DVI-D	Dual Link DVI-D	N	2 port Single DVI 4K video Secure KVM without CAC PP3.0
SV142H1	4	Single	DisplayPort	HDMI	Y	4 Port Single DP-HDMI 4K video Secure KVM with CAC PP3.0
SV142H0	4	Single	DisplayPort	HDMI	N	4 Port Single DP-HDMI 4K video Secure KVM without CAC PP3.0
SV242H1	4	Dual	DisplayPort	HDMI	Y	4 Port Dual DP-HDMI 4K video Secure KVM with CAC PP3.0
SV242H0	4	Dual	DisplayPort	HDMI	N	4 Port Dual DP-HDMI Secure KVM without CAC PP3.0
SV142P1	4	Single	DisplayPort	DisplayPort	Y	4 port Single DP to DP 4K video Secure KVM with CAC PP3.0
SV142P0	4	Single	DisplayPort	DisplayPort	N	4 port Single DP to DP 4K video Secure KVM without CAC PP3.0
SV122P1	2	Single	DisplayPort	DisplayPort	Y	2 port Single DP to DP 4K video SKVM with CAC PP3.0
SV122P0	2	Single	DisplayPort	DisplayPort	N	2 port Single DP to DP 4K video Secure KVM without CAC PP3.0
SV242P1	4	Dual	DisplayPort	DisplayPort	Y	4 port Dual DP to DP 4K video Secure KVM with CAC PP3.0
SV242P0	4	Dual	DisplayPort	DisplayPort	N	4 port Dual DP to DP 4K video Secure KVM without CAC PP3.0
SV222P1	2	Dual	DisplayPort	DisplayPort	Y	2 port Dual DP to DP 4K video Secure KVM with CAC PP3.0
SV222P0	2	Dual	DisplayPort	DisplayPort	N	2 port Dual DP to DP 4K video Secure KVM without CAC PP3.0

1.5.2 TOE Logical Boundaries

The logical boundary of the TOE includes those security functions implemented exclusively by the TOE. These security functions are identified in Section 1.4.3 above and are further described in the following subsections. A more detailed description of the implementation of these security functions are provided in Section 7 “TOE Summary Specification”.

1.5.2.1 User Data Protection and Data Isolation

The TOE switches one peripheral group between two or four (depending on model) computer port groups. The TOE filters USB devices to ensure that only Human Interface Devices (HID) and CAC Readers are allowed. The TOE ensures the peripheral group is only connected to a single computer port group at a time and prevents the computer port groups to communicate with each other through the TOE.

The TOE indicates which computer port group is selected using LEDs on the front of the KVM or DCU and only changes the selected computer port group when the user presses the button for a different channel.

1.5.2.2 Protection of the TSF

The TOE utilizes tamper labels and tamper switches to indicate and respond to the enclosure being opened. If the KVM or DCU enclosure is opened, the TOE overwrites a portion of its firmware to permanently disable the TOE.

The TOE runs a suite of self-tests to check the integrity of the hardware and firmware. The self-tests also check to see if one of the selector buttons is stuck. If any self-tests fail, the TOE enters a warning mode and will not connect the peripheral group to any computer group.

1.5.2.3 TOE Access

When the TOE powers-up, it defaults to selecting computer group 1. The TOE also removes power from the CAC reader when the selected computer is changed to ensure the any authentication sessions are cleared.

1.6 Notation, formatting, and conventions

The notation, formatting, and conventions used in this Security Target are defined below; these styles and clarifying information conventions were developed to aid the reader.

Where necessary, the ST author has added application notes to provide the reader with additional details to aid understanding; they are italicized and usually appear following the element needing clarification. Those notes specific to the TOE are marked “ST Application Note;” those taken from the Protection Profile are marked “Application Note.”

The notation conventions that refer to iterations, assignments, selections, and refinements made in this Security Target are in reference to SARs and SFRs taken directly from CC Part 2 and Part 3 as well as any SFRs and SARs taken from a Protection Profile.

The notation used in those PP to indicate iterations, assignments, selections, and refinements of SARs and SFRs taken from CC Part 2 and Part 3 is not carried forward into this document. Additionally, obvious errors in the PP are corrected and noted as such.

The CC permits four component operations (assignment, iteration, refinement, and selection) to be performed on requirement components. These operations are defined in Common Criteria, Part 1; paragraph 6.4.1.3.2, “Permitted operations on components” as:

- Iteration: allows a component to be used more than once with varying operations;
- Assignment: allows the specification of parameters;
- Selection: allows the specification of one or more items from a list; and

- Refinement: allows the addition of details.

Iterations are indicated by a number in parenthesis following the requirement number, e.g., FIA_UAU.1.1(1); the iterated requirement titles are similarly indicated, e.g., FIA_UAU.1(1).

Assignments made by the ST author are identified with **bold text.**

Selections are identified with underlined text**.**

Refinements that add text use ***bold and italicized text*** to identified the added text**.** Refinements that performs a deletion, identifies the deleted text with ~~***strikeout, bold, and italicized text***~~.

2 Conformance Claims

2.1 Common Criteria Conformance Claims

This Security Target is conformant to the Common Criteria Version 3.1r4, CC Part 2 extended [C2], and CC Part 3 conformant [C3].

2.2 Conformance to Protection Profiles

This Security Target claims exact compliance to the collaborative Protection Profile for Peripheral Sharing Switch, Version 3.0, dated February 13, 2015 [PSS]. This Protection Profile will be referred to as PSS or PP for convenience throughout this Security Target.

The TOE complies with the following Technical Decisions:

- TD0298: Update to FDP_RIP.1 Assurance Activities
- TD0144: FDP_RIP.1.1 - Purge Memory and Restore Factory Defaults Optional
- TD0136: FDP_RIP.1.1 - Refinement
- TD0086: DisplayPort to HDMI Conversion Functionality
- TD0083: Vulnerability Survey Assurance Component (AVA_VAN.1) in PSS PP v3.0

2.3 Conformance to Security Packages

This Security Target does not claim conformance to any security function requirements or security assurance requirements packages, neither as package-conformant or package-augmented.

2.4 Conformance Claims Rationale

To demonstrate that exact conformance is met, this rationale shows all threats are addressed, all OSP are satisfied, no additional assumptions are made, all objectives have been addressed, and all SFRs and SARs have been instantiated.

The following address the completeness of the threats, OSP, and objectives, limitations on the assumptions, and instantiation of the SFRs and SARs:

- Threats
  - All threats defined in the PSS are carried forward to this ST;
  - No additional threats have been defined in this ST.
- Organizational Security Policies
  - All OSP defined in the PSS are carried forward to this ST;

- No additional OSPs have been defined in this ST.

- Assumptions
  - All assumptions defined in the PSS are carried forward to this ST;
  - No additional assumptions for the operational environment have been defined in this ST.
- Objectives
  - All objectives defined in the PSS are carried forward to this ST.
- All SFRs and SARs defined in the PSS are carried forward to this Security Target.

Rationale presented in the body of this ST shows all assumptions on the operational environment have been upheld, all the OSP are enforced, all defined objectives have been met and these objectives counter the defined threats.

Additionally, all SFRs and SARs defined in the PSS have been properly instantiated in this Security Target; therefore, this ST shows exact conformance to the PSS.

3 Security Problem Definition

3.1 Threats

The following table defines the security threats for the TOE, characterized by a threat agent, an asset, and an adverse action of that threat agent on that asset. These threats are taken directly from the PP unchanged.

Table 2: Threats

Threat	Description
T.DATA_LEAK	A connection via the PSS between computers may allow unauthorized data flow through the PSS or its connected peripherals.
T.SIGNAL_LEAK	A connection via the PSS between computers may allow unauthorized data flow through bit-by-bit signaling.
T.RESIDUAL_LEAK	A PSS may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer. More specifically, a PSS may leak user keyboard entries to a PSS-connected computer other than the selected computer in real-time or at a later time.
T.UNINTENDED_SWITCHING	A threat in which the user is connected to a computer other than the one to which the user intended to be connected.
T.UNAUTHORIZED_DEVICES	The use of an unauthorized peripheral device with a specific PSS peripheral port may allow unauthorized data flows between connected devices or enable an attack on the PSS or its connected computers.
T.AUTHORIZED_BUT_UNTRUSTED_DEVICES	The use of an authorized peripheral device with the PSS may still cause unauthorized data flows between connected devices or enable an attack on the PSS or its connected computers. Such threats are possible due to known or unknown device vulnerabilities or due to additional functions within the authorized peripheral device.
T.MICROPHONE_USE	Microphone connected to the TOE used for audio eavesdropping or to transfer data across an air-gap through audio signaling.
T.AUDIO_REVERSED	Audio output device used by an attacker as a low-gain microphone for audio eavesdropping. This threat is an abuse of the computer and TOE audio output path to reverse the analog data flow from the headphones to the computer. The computer then amplifies and filters the weak signal, and then digitizes and streams it to another location.
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 embedded in the TOE's volatile or non-volatile memory to allow unauthorized information flows between connected devices.
T.PHYSICAL_TAMPER	A malicious human agent could physically tamper with or modify the TOE to allow unauthorized information flows between connected devices.
T.REPLACEMENT	A malicious human agent could replace the TOE during shipping, storage, or use with an alternate device that does not enforce the TOE security policies.
T.FAILED	Detectable failure of a PSS may cause an unauthorized information flow, weakening of PSS security functions, or unintended switching.

3.2 Assumptions

This section describes the assumptions on the operational environment in which the TOE is intended to be used. It includes information about the physical, personnel, and connectivity aspects of the environment. The operational environment must be managed in accordance with the provided guidance documentation. The following table defines specific conditions that are assumed to exist in an environment where the TOE is deployed. These assumptions are taken directly from the PP unchanged.

Table 3: Assumptions

Assumption	Description
A.NO_TEMPEST	It is assumed that the computers and peripheral devices connected to the TOE are not TEMPEST approved.

Table 3: Assumptions

Assumption	Description
A.NO_SPECIAL_ANALOG_CAPABILITIES	It is assumed that the computers connected to the TOE are not equipped with special analog data collection cards or peripherals such as: Analog to digital interface, high performance audio interface, Digital Signal Processing function, and analog video capture function.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators and users are trusted to follow and apply all guidance in a trusted manner.
A.TRUSTED_CONFIG	Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

4 Security Objectives

4.1 Security Objectives for the TOE

Table 4: Security Objectives for the TOE

Objective	Description
O.COMPUTER_INTERFACE_ISOLATION	The TOE must prevent unauthorized data flow to assure that the TOE and/or its connected peripheral devices would not be exploited in an attempt to leak data. The TOE computer interface shall be isolated from all other TOE computer interfaces while TOE is powered.
O.COMPUTER_INTERFACE_ISOLATION_ TOE_UNPOWERED	The same level of isolation defined in the dataflow objectives must be maintained at all times, including periods while TOE is unpowered.
O.USER_DATA_ISOLATION	User data such as keyboard entries should be switched (i.e., routed) by the TOE only to the computer selected by the user. The TOE must provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.
O.NO_USER_DATA_RETENTION	The TOE shall not retain user data after it is powered down.
O.PURGE_TOE_KB_DATA_WHILE_ SWITCHING	The TOE shall purge all user keyboard data from computer interfaces following channel switching and before interacting with the new connected computer.
O.NO_DOCKING_PROTOCOLS	The use of docking protocols such as DockPort, USB docking, Thunderbolt etc. is not allowed in the TOE.
O.NO_OTHER_EXTERNAL_INTERFACES	The TOE may not have any wired or wireless external interface with external entities (external entity is an entity outside the TOE evaluated system, its connected computers and peripheral devices).
O.NO_ANALOG_AUDIO_INPUT	Shared audio input peripheral functions (i.e., analog audio microphone input or line input) are not allowed in the TOE
O.UNIDIRECTIONAL_AUDIO_OUT	The TOE shall be designed to assure that reverse audio signal attenuation will be at least 30 dBv measured with 200 mV and 2V input pure sine wave at the extended audio frequency range including negative swing signal. The level of the reverse audio signal received by the selected computer shall be minimal to assure that the signal level generated by headphones will be well under the noise floor level.
O.COMPUTER_TO_AUDIO_ISOLATION	The audio dataflow shall be isolated from all other TOE functions. Signal attenuation between any TOE computer interface and any TOE audio interface shall be at least 45 dBv measured with 2V input pure sine wave at the extended audio frequency range including negative swing signal.
O.USER_AUTHENTICATION_ISOLATION	The user authentication function shall be isolated from all other TOE functions.
O.USER_AUTHENTICATION_RESET	Unless the TOE emulating the user authentication function, upon switching computers, the TOE shall reset (turn off and then turn on) the power supplied to the user authentication device for at least 1 second.
O.USER_AUTHENTICATION_ TERMINATION	If the TOE is emulating the user authentication (instances of the user authentication device are coupled to multiple computers at the same time) then once the authentication session is terminated.
~~O.USER_AUTHENTICATION_ADMIN~~	~~If the TOE is capable of being configured after deployment with user authentication device qualification parameters then such configuration may only performed by an administrator.~~
O.AUTHORIZED_SWITCHING	The TOE shall allow only authorized switching mechanisms to switch between connected computers and shall explicitly prohibit or ignore unauthorized switching mechanisms.
O.NO_AMBIGUOUS_CONTROL	If the TOE allows more than one authorized switching mechanism, only one method shall be operative at any given time to prevent ambiguous commands.

Table 4: Security Objectives for the TOE

Objective	Description
O.CONTINUOUS_INDICATION	The TOE shall provide continuous visual indication of the computer to which the user is currently connected.
O.KEYBOARD_AND_MOUSE_TIED	The TOE shall ensure that the keyboard and mouse devices are always switched together
O.NO_CONNECTED_COMPUTER_ CONTROL	The TOE shall not allow TOE control through a connected computer.
O.PERIPHERAL_PORTS_ISOLATION	The TOE shall prevent data flow between peripheral devices of different SPFs and the TOE peripheral device ports of different SPFs shall be isolated.
O.DISABLE_UNAUTHORIZED_ PERIPHERAL	The TOE shall only allow authorized peripheral device types (See Annex C) per peripheral device port; all other devices shall be identified and then rejected or ignored by the TOE.
O.DISABLE_UNAUTHORIZED_ ENDPOINTS	The TOE shall reject unauthorized peripheral devices connected via a USB hub. Alternatively, the TOE may reject all USB hubs.
O.KEYBOARD_MOUSE_EMULATED	The TOE keyboard and pointing device functions shall be emulated (i.e., no electrical connection other than the common ground is allowed between peripheral devices and connected computers).
O.KEYBOARD_MOUSE_UNIDIRECTIONAL	The TOE keyboard and pointing device data shall be forced to unidirectional flow from the peripheral device to the switched computer only.
O.UNIDIRECTIONAL_VIDEO	TOEs that support VGA, DVI or HDMI video shall force native video peripheral data (i.e., red, green, blue, and TMDS lines) to unidirectional flow from the switched computer to the connected display device.
O.UNIDIRERCTIONAL_EDID	TOEs that support VGA, DVI, DisplayPort or HDMI video shall force the display EDID peripheral data channel to unidirectional flow and only copy once from the display to each one of the appropriate computer interfaces during the TOE power up or reboot sequence. The TOE must prevent any EDID channel write transactions initiated by connected computers.
O.DISPLAYPORT_AUX_FILTERING	TOEs that support DisplayPort video shall prevent (i.e., filter or otherwise disable) the following auxiliary channel traffic: EDID write, USB, Ethernet, Audio return channel, UART and MCCS. Alternatively, the TOE may prevent the AUX channel from operating at Fast AUX speed (675/720 Mbps).
O.TAMPER_EVIDENT_LABEL	The TOE 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 TOE and continue to be available during the TOE deployment. The TOE shall be labeled with at least one visible unique identifying tamper-evident marking that can be used to authenticate the device. The TOE manufacturer must maintain a complete list of manufactured TOE articles and their respective identification markings' unique identifiers.
O.ANTI_TAMPERING	The TOE shall be physically enclosed so that any attempts to open or otherwise access the internals or modify the connections of the TOE would be evident. This shall be accomplished through the use of an always-on active anti-tampering system that serves to permanently disable the TOE should its enclosure be opened. The TOE shall use an always-on active anti-tampering system to permanently disable the TOE in case physical tampering is detected.
O.ANTI_TAMPERING_BACKUP_POWER	The anti-tampering system must have a backup power source to enable tamper detection while the TOE is unpowered.
O.ANTI_TAMPERING_BACKUP_FAIL_ TRIGGER	A failure or depletion of the anti-tampering system backup power source shall trigger TOE to enter tampered state.
O.ANTI_TAMPERING_INDICATION	The TOE shall have clear user indications when tampering is detected.

Table 4: Security Objectives for the TOE

Objective	Description
O.ANTI_TAMPERING_PERMANENTLY_ DISABLE_TOE	Once the TOE anti-tampering is triggered, the TOE shall become permanently disabled. No peripheral-to-computer data flows shall be allowed.
O.NO_TOE_ACCESS	The TOE shall be designed so that access to the TOE firmware, software, or its memory via its accessible ports is prevented.
O.SELF_TEST	The TOE shall perform self-tests following power up or powered reset.
O.SELF_TEST_FAIL_TOE_DISABLE	Upon critical failure detection the TOE shall disable normal operation of the whole TOE or the respective failed component.
O.SELF_TEST_FAIL_INDICATION	The TOE shall provide clear and visible user indications in the case of a self-test failure.

4.2 Security Objectives for the Operational Environment

Table 5: Security Objectives for the Operational Environment

Objective	Description
OE. NO_TEMPEST	The operational environment will not require the use of TEMPEST approved equipment.
OE. NO_SPECIAL_ANALOG_CAPABILITIES	The operational environment will not require special analog data collection cards or peripherals such as: Analog to digital interface, high performance audio interface, Digital Signal Processing function, and analog video capture function.
OE.PHYSICAL	The operational environment will provide physical security, commensurate with the value of the TOE and the data it contains.
OE.TRUSTED_ADMIN	The operational environment will ensure that appropriately trained and trusted TOE Administrators and users are available to administer, configure and use the TOE.

5 Extended Components Definition

This section provides definition of the extended security functional and assurance requirements; the components that are CC Part 2 extended.

5.1 Extended Security Functional Requirements Definitions

There are no extended Security Functional Requirements defined in this Security Target. All extended SFRs are defined in the [PSS] Annex H.

6 Security Requirements

This section describes the security functional and assurance requirements for the TOE; those that are CC Part 2 conformant, CC Part 2 extended, and CC Part 3 conformant.

6.1 Security Function Requirements

This section describes the functional requirements for the TOE. The security functional requirement components in this security target are CC Part 2 conformant or CC Part 2 extended as defined in Section 2, Conformance Claims. Operations that were performed in [PSS] are not signified in this section. Operations performed by the ST are denoted according to the formatting conventions in Section 1.6.

Table 6: Security Functional Requirements

# SFR	Description
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.1 (1)	Subset information flow control
FDP_IFC.1 (2)	Subset information flow control
FDP_IFF.1 (1)	Information flow control functions
FDP_IFF.1 (2)	Simple security attributes
FDP_RIP.1 (1)	Subset Residual information protection
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.1	Passive detection of a physical attack
FPT_PHP.3	Resistance to physical attack
FPT_TST.1	TSF testing
FTA_ATH_EXT.1	User authentication device reset
FTA_CIN_EXT.1	Extended: Continuous Indications

6.1.1 Class FDP: User Data Protection

6.1.1.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1

The TSF shall enforce the peripheral device SFP on

- Subjects: Peripheral devices
- Objects: Console ports
- Operations: allow connection, disallow connection.

6.1.1.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1

The TSF shall enforce the peripheral device SFP to objects based on the following:

- Subjects: Peripheral devices
  - Subject security attributes: peripheral device type

- Objects: Console ports
  - Object security attributes: none.

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: The TOE shall query the connected peripheral device upon initial connection or upon TOE power up and allow connection for authorized peripheral devices in accordance with the table in Annex C of the PP.

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: The TOE peripheral device interface (console) port shall reject any peripheral device with unauthorized values.

6.1.1.3 FDP_IFC.1(1) Subset information flow control

FDP_IFC.1.1(1)

The TSF shall enforce the User Data Protection SFP on

- Subjects: TOE computer interfaces, TOE peripheral device interfaces
- Information: User data transiting the TOE
- Operations: Data flow between subjects.

6.1.1.4 FDP_IFC.1(2) Subset information flow control

FDP_IFC.1.1(2)

The TSF shall enforce the Data Isolation SFP on

- Subjects: TOE computer interfaces, TOE peripheral interfaces
- Information: data transiting the TOE
- Operations: data flows between computer interfaces.

Application Notes:

The Data Isolation SFP shall be enforced on data transiting the TOE wherein this data may be:

a. User data – this is typically text typed by the user on the connected keyboard, but may be other types of user information, such as display video; and

b. Other data transiting the TOE – a generalized view of data that may be the result of a hostile action attributable to a threat agent acting from within one or more of the TOE connected computers.

It should be noted that data transiting the TOE does not refer to data generated by the TOE such as TOE monitoring or control information (for example: user selected computer number or name).

6.1.1.5 FDP_IFF.1(1) Simple security attributes

FDP_IFF.1.1(1)

The TSF shall enforce the User Data Protection SFP based on the following types of subject and information security attributes:

- Subject: TOE computer interfaces
    - Subject security attributes: user selected computer interface
- Subject: TOE peripheral device interfaces
    - Subject security attributes: none
- Information: User data transiting the TOE
    - Information security attributes: none.

FDP_IFF.1.2(1)

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: The user makes a selection to establish a data flow connection between the peripheral device interfaces and one computer interface based on the following rules:

1. The attribute User Selected Computer determines the operation Allowed Data Flow such that the only permitted data flows are as listed in the table below:

Value of User Selected Computer	Allowed Data Flow
n	User keyboard peripheral device interface data flowing from peripheral device interface to computer interface #n; User mouse peripheral device interface data flowing from peripheral device interface to computer interface #n; User display peripheral device interface data flowing from computer interface #1 to one or more user display peripheral device interfaces; User authentication peripheral device data flowing bidirectional between computer interface #n and user authentication device peripheral interface; Analog audio output data flowing from computer interface #n to the audio peripheral device interface

2. When the user changes the attribute by selecting a different computer, this causes the TOE to change the data flow accordingly.

FDP_IFF.1.3(1)

The TSF shall enforce the following additional information flow control SFP rules if the TOE supports user authentication devices: following an event of the user changing the attribute by selecting a different computer, the TOE must reset the power to the connected user authentication device.

FDP_IFF.1.4(1)

The TSF shall explicitly authorize an information flow based on the following rules: no additional rules.

FDP_IFF.1.5(1)

The TSF shall explicitly deny an information flow based on the following rules:

1. The TSF shall deny any information flow between TOE peripheral device interfaces and TOE non-selected computer interfaces.

2. The TSF shall deny any data flow between an external entity and the TOE computer interfaces.

3. The TSF shall deny any user data flow between the TOE and an external entity.

Application Notes:

Note that an external entity is any device that is not part of the evaluated TOE system, its connected computers or connected peripheral devices.

Therefore, with regard to data flow between the TOE and an external entity:

a. TOE status information such as currently selected computer number or firmware version is not user data and therefore may be transmitted to other (external) entities;

b. KVM cables, extenders or adapters connected to a TOE computer interface or to a peripheral interface are not considered external entities and are therefore excluded from this requirement.

6.1.1.6 FDP_IFF.1(2) Simple security attributes

FDP_IFF.1.1(2)

The TSF shall enforce the Data Isolation SFP based on the following types of subject and information security attributes:

- Subject: TOE interfaces
    - Subject security attributes: Interface types (Allowed TOE interface types are listed in Annex C of the PP. Power source and connected computer interfaces are also applicable interface types.)
- Subject: TOE peripheral device interfaces
    - Subject security attributes: none
- Information: data transiting the TOE
    - Information security attributes: data types. (The TSF shall enforce the data isolation SFP on the following data types:
        a. User keyboard key codes;
        b. User pointing device commands;
        c. Video information (User display video data and display management data);
        d. Audio output data; and
        e. User authentication device data.).

FDP_IFF.1.2(2)

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

1. During normal TOE operation, the TSF shall permit only user entered keyboard key codes, and user input mouse commands to flow between the TOE keyboard and mouse peripheral device interfaces and the TOE selected computer interface. No flow is permitted between the selected computer interface and the TOE keyboard and mouse peripheral device interfaces.

2. The TSF shall permit information flow and TSF resources sharing between two TOE user peripheral interfaces of the same Shared Peripheral group. Both functions may share the same interface.

Application Notes:

A Shared Peripheral group refers to user peripherals that are switched together as a group. For example, the user keyboard and user mouse shall be switched together and are therefore in the same Shared Peripheral group.

Data flow between the keyboard and the mouse peripheral interfaces is allowed (ports can be shared or interchangeable).

Normal TOE operation occurs at any time when the TOE is powered on and it is not:

a. Initializing; or

b. In self-test; or

c. Being configured; or

d. In tampered state; or

e. In self-test failed state.

FDP_IFF.1.3(2) The TSF shall enforce the No additional rules.

FDP_IFF.1.4(2) The TSF shall explicitly authorize an information flow based on the following rules: No additional rules.

FDP_IFF.1.5(2) The TSF shall explicitly deny an information flow based on the following rules:

1. The TSF shall deny any information flow between TOE Computer Interfaces, except those allowed by the User Data Flow rules;
2. The TSF shall deny data flow other than keyboard entries and mouse reports between the TOE keyboard and mouse peripheral device interfaces and the TOE selected computer interface;
3. The TSF shall deny power flow between the selected computer interface and TOE keyboard and mouse peripheral device interfaces;
4. The TSF shall deny information flow from the TOE selected computer interface to the TOE keyboard and mouse peripheral device interface;
5. The TSF shall deny data flow of user authentication device data transiting the TOE to non-selected TOE computer interfaces;
6. The TSF shall assure that the user authentication device computer interfaces are not shared with any other TOE peripheral function interface (keyboard, mouse etc.);
7. The TSF shall deny information flow between two TOE user peripheral interfaces in different Shared Peripheral groups;
8. The TSF shall deny analog audio information flow between the TOE selected computer audio interface and the user audio device peripheral interface when a microphone peripheral device is intentionally or unintentionally connected to the TOE audio peripheral device interface;
9. The TSF shall enforce unidirectional information flow between the TOE selected computer audio interface and the user audio device peripheral interface. Bidirectional information flow shall be denied;
10. The TSF shall deny all AUX Channel information flows other than link negotiation, link training and EDID reading;

11. The TSF shall deny any information flow from the TOE display peripheral device interface and the selected computer interface with the exception of EDID information that may be passed once at TOE power up or after recovery from TOE reset;
12. The TSF shall deny an information flow between the selected computer display interface and the TOE display peripheral device interface on the EDID channel;
13. The TSF shall recognize and enable only those peripherals with an authorized interface type as defined in Annex C of the PP. Information flow to all other peripherals shall be denied; and
14. All denied information flows shall also be denied when the TOE's power source is removed.

6.1.1.7 FDP_RIP.1(1) Subset residual information protection

FDP_RIP.1.1(1)

The TSF shall ensure that any previous information content of a resource is made unavailable

- immediately after TOE switch to another selected computer;
- and on start-up of the TOE for

the following objects: a TOE computer interface.

ST Application Notes:

FDP_RIP.1.1(1) was updated as specified by TD0136.

FDP_RIP.1.1(1) was iterated as specified by TD0144.

6.1.2 Class FPT: Protection of the TSF

6.1.2.1 FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1

The TSF shall preserve a secure state by disabling the TOE when the following types of failures occur: failure of the power on self-test, failure of the anti-tampering function.

6.1.2.2 FPT_PHP.1 Passive detection of a 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.

6.1.2.3 FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1

The TSF shall resist a physical attack on the TOE for the purpose of gaining access to the internal components, or to damage the anti-tampering battery to the TOE Enclosure by becoming permanently disabled.

Application Notes:

'Becoming permanently disabled' is interpreted to mean that all connected peripheral devices shall not function.

The design of the TOE enclosure and anti-tampering functions shall assure that any attempt to open the enclosure enough to allow access to the internal components will activate the anti-tampering function.

6.1.2.4 FPT_TST.1 TSF testing

FPT_TST.1.1

The TSF shall run a suite of self-tests that includes as minimum:

a. Test of the basic TOE hardware and firmware integrity; and

b. Test of the basic computer-to-computer isolation; and

c. Test of critical security functions (i.e., user control and anti-tampering).

during initial startup, upon reset button activation to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide users with the capability to verify the integrity of the TSF functionality.

FPT_TST.1.3 The TSF shall provide users with the capability to verify the integrity of the TSF.

6.1.3 Class FTA: TOE Access

6.1.3.1 FTA_ATH_EXT.1 User authentication device reset

FTA_ATH_EXT.1.1

The TSF shall reset the power supplied to the user authentication device for at least one second when the user switches the device from one computer to another.

6.1.3.2 FTA_CIN_EXT.1 Extended: Continuous Indications

FTA_CIN_EXT.1.1

The TSF shall display a continuous visual indication of the computer to which the user is currently connected, including on power up.

6.2 Security Assurance Requirements

The TOE meets the assurance requirements specified in the "Assurance Activities" subsections of Section 4 of the [PSS].

6.2.1 Class AVA: Vulnerability Assessment

6.2.1.1 Vulnerability Survey (AVA_VAN.1)

This component is targeted at identifying the TOE such that it can be distinguished from other products or versions from the same vendor and can be easily specified when being procured by an end user. The TOE will have additional labeling requirements to meet the demands of FPT_PHP.1.

Developer action elements:

AVA_VAN.1.1D	The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.1.1C	The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence
AVA_VAN.1.2E	The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE
AVA_VAN.1.3E	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

ST Application Note:

AVA_VAN.1 was added as specified by TD0083.

7 TOE Summary Specification

This section provides evaluators and potential consumers of the TOE with a high-level description of each SFR, thereby enabling them to gain a general understanding of how the TOE is implemented. These descriptions are intentionally not overly detailed, thereby disclosing no proprietary information. These sections refer to SFRs defined in Section 6, Security Requirements.

The TOE consists of the following Security Functions:

- User Data Protection and Data Isolation
- Protection of the TSF
- TOE Access

7.1 User Data Protection and Data Isolation

The KMV supports the following physical ports:

- 2 or 4 Computer Port Groups
  - 1x or 2x Display (Dual Link DVI-D v1.0 or DisplayPort v1.2a)
  - 1x Mouse/Keyboard (USB 2.0 Type B)
  - 0x or 1x CAC (USB 2.0 Type B)
  - 1x Analog Audio Input (3.5mm)
- 1 Peripheral Group
  - 1x or 2x Display (Dual Link DVI-D v1.0, DisplayPort v1.2a, or HDMI v1.4)
  - 1x Mouse (USB Type A)
  - 1x Mouse (PS/2)
  - 1x Keyboard (USB Type A)
  - 1x Keyboard (PS/2)
  - 0x or 1x CAC (USB 2.0 Type A)
  - 1x Analog Audio Output (3.5mm)
- Other Ports
  - 1x DC Power Input
  - 1x DCU port

The DCU supports the following physical port:

- 1x DCU port

A dedicated cable connects the KVM component of the TOE to the DCU component of the TOE. The exact Display and CAC ports supported are identified in Table 1.

The switched peripheral group always connected to a single computer. To further isolate the switched peripheral group from the connected computer port group, the TOE provides the following protections: provides USB power, unidirectional video, and unidirectional audio.

The TOE provides USB power protection by powering USB peripherals from the TOE's power adapter. This prevents USB power signal leakage back to the computer port groups.

The TOE only connects the video signal between the selected computer and display; it does not connect the bi-directional data channel (e.g. DisplayPort AUX, DVI/HDMI DDC). The TOE reads the EDID from the display when the TOE is powered on and emulates a display when a connected computer requests the EDID. The TOE disassembles bi-directional data requests and does not process any requests except for EDID requests.

The TOE provides the unidirectional audio protection using analog to digital converters connected to the Analog Audio Input ports and a digital to analog converter connected to the Analog Audit Output port.

The TOE does not support any wireless interfaces and is conformant with radiated emissions requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A.

When the TOE consists of the KVM only, the user invokes the switching by pressing the button on the front panel of the KVM that corresponds to the desired computer port group. When the TOE consists of the KVM and DCU, the user invokes the switching by pressing a button on the DCU that corresponds to the desired computer port group.

FDP_IFC.1(1), FDP_IFF.1(1), FDP_IFC.1(2), FPD_IFF.1(2), FDP_ACC.1, FDP_ACF.1

7.1.1 USB Filtering

The TOE performs the following filtering for all USB devices by querying the following attributes and descriptors from endpoint 0:

- Verify the device only supports one configuration checking the bNumConfigurations in the DeviceDescriptor.
- Verify bit 6 in the bmAttribute field in the ConfigurationDescriptor is 0 (i.e. bus powered).
- Verify the bInterfaceClass and bInterfaceProtocol for each InterfaceDescriptor as described below.

On TOE models with a CAC port (see Table 1), the TOE filters USB devices connected to this port as described above and verifying the bInterfaceClass is 0x0B (SmartCard/CAC) and the bInterfaceProtocol is 0x00 (Chip Card Interface Device) This restriction is hard coded into the TOE during manufacturing. The TOE does not emulate the authentication device. When the selected computer port group is changed, the TOE disconnects the authentication device from the previously selected computer, removes power from the authentication device for 1 second, reapplies power, and connects the authentication device to the selected computer port group. The TOE also allows the operator to slide a switch on the KVM to enable/disable the CAC connection to any computer port group. When the CAC switch is disabled for the selected computer port group, the TOE does not connect the CAC Peripheral Port to the selected Computer Port. The TOE contains separate data and power lines for the USB authentication device and the USB HID devices.

The TOE has USB Mouse and Keyboard ports in the switched peripheral group are interchangeable. The TOE filters USB devices connected to either of these ports as described above and verifying the bInterfaceClass is 0x03 (HID) and bInterfaceProtocol is 0x01 (Keyboard) or 0x02 (Mouse). Composite HID devices are supported.

If a USB device fails any of the checks described in this section, the TOE disables the device and prevents any data flowing to/from any of the endpoints in the device.

FDP_IFC.1(1), FDP_IFF.1(1), FDP_IFC.1(2), FPD_IFF.1(2), FDP_ACC.1, FDP_ACF.1

7.1.2 Letter of Volatility

The following table is the TOE’s Letter of Volatility. All of the memory devices are powered by the TOE.

Table 7: Letter of Volatility

Part	PN	Manufacturer	Memory Type	Size	User Data
System Controller	LPC1833JBD144	NXP Semiconductors	SRAM (Volatile)	136KB	No
			Flash (Non-volatile)	512KB	No

(KVM with CAC)			EEPROM (Non-volatile)	16KB	No
System Controller (KVM without CAC)	EFM8UB20F64G-B-QFP48	Silicon Labs	RAM (Volatile)	4352B	No
			Flash (Non-volatile)	64KB	No
Host Emulator (KVM)	LPC1833JBD144	NXP Semiconductors	SRAM (Volatile)	136KB	Yes
			Flash (Non-volatile)	512KB	No
			EEPROM (Non-volatile)	16KB	No
Device Emulators (KVM)	EFM8UB10F16G-C-QFN20	Silicon Labs	RAM (Volatile)	2304B	Yes
			Flash (Non-volatile)	16KB	No
Real Time Clock (KVM)	ISL1208	Intersilisl	SRAM (Volatile)	2B	No
Master EDID Emulator (KVM)	EFM8UB10F16G-C-QFN20	Silicon Labs	RAM (Volatile)	2304B	Yes
			Flash (Non-volatile)	16KB	No
Device EDID Emulators (KVM)	EFM8UB10F16G-C-QFN20	Silicon Labs	RAM (Volatile)	2304B	Yes
			Flash (Non-volatile)	16KB	No
Switch Controller (KVM)	EFM8UB10F16G-C-QFN20	Silicon Labs	RAM (Volatile)	2304B	Yes
			Flash (Non-volatile)	16KB	No
System Controller (DCU)	EFM8UB10F16G-C-QFN28	Silicon Labs	RAM (Volatile)	2304B	Yes
			Flash (Non-volatile)	16KB	No
Real Time Clock (DCU)	ISL1208	Intersilisl	SRAM (Volatile)	2B	No

FDP_RIP.1(1)

7.2 Protection of the TSF

The TSF allows the user to determine if the TOE enclosure has been opened by inspecting three tamper labels (one on the top/front, one on the rear/right covering a mounting screw, and one on the rear/left covering a mounting screw) on the KVM component of the TOE and a single tamper label on the DCU component of the TOE. Each tamper label has a holographic background, a unique serial number, and strong adhesive. The strong adhesive makes the tamper labels difficult to remove and provides a high likelihood that removal will cause visible tears in the holographic image.

FPT_PHP.1

Both the KVM and DCU components of the TOE include an active tamper detection mechanism. If either enclosure is opened, the tamper switch is triggered, and the component permanently disables itself by overwriting the firmware containing the normal TOE functionality, only leaving the tamper indication functionality. The tamper state propagates (triggers the KVM tamper mechanism) from the DCU to the KVM when the TOE has power (both continuously powered and at powered up). The tamper state does not propagate from the KVM to the DCU under any conditions, because the TOE cannot transfer any user data or bypass data isolation when the KVM is tampered.

The TOE utilizes the microcontroller's Code Read Protection features to disable the JTAG interface and disable all firmware read/write capabilities from outside the microcontroller. If either component of the TOE detects its battery powering the anti-tamper mechanism is nearly exhausted, the TOE activates the anti-tamper mechanism.

When the TOE has been tampered, the TOE indicates tamper by sequentially blinking the channel selection LEDs on the KVM and DCU (e.g. CH1 LED -> CH2 LED -> CH3 LED -> CH4 LED).

FPT_PHP.3

The TSF performs the following self-tests automatically when power is applied:

- The KVM component of the TOE checks the HW by performing a roll call to each channel selector IC. The microcontroller sends a pattern to each channel selector IC and verifies the IC sends the same pattern in response.
- The TOE (both KVM and DCU components) verifies a CRC32 checksum to verify the integrity of the firmware.
- The KVM component of the TOE checks the computer isolation by sending a special key code to each HID emulator. The TOE verifies the intended HID emulator receives the key code and none of the unintended HID emulators receive the key code.
- The TOE (both KVM and DCU components) checks the voltage of the batteries for the anti-tampering mechanism. If the battery voltage is low for either component, the TOE activates the anti-tamper mechanisms.
- The TOE HW (both KVM and DCU components) is also tested runs a Sticky Button Test which checks if a channel selection button is continuously depressed for 100 ms during power-up. If a button is detected to be continually depressed, this test fails due to a possible short or mechanical issue.

If any of the self-tests fail, the TOE disables all PSS functionality and enters a warning mode. The TOE simultaneously flashes all of the LEDs on the KVM and DCU to indicate the TOE has encountered an error. The user can re-run self-tests by disconnecting and reconnecting power from the TOE. If the self-tests pass, the TOE will resume normal operation.

FPT_TST.1, FPT_FLS.1

7.3 TOE Access

The KVM component of the TOE contains two or four LEDs (depending on the model) on the front panel to indicate currently selected channel. The KVM component of the TOE that include a CAC port also contain two or four LEDs to indicate if the CAC port is active on the selected channel. The LEDs on the KVM also indicate tamper and self-test failures as described in Section 7.2.

The DCU component of the TOE contains four LEDs on the front panel to indicate currently selected channel as well as four LEDs to indicate if the CAC port is active. When the DCU is connected to a KVM that does not support four ports and/or CAC, the additional LEDs remain inactive on the DCU.

When power is applied to the TOE, the TOE runs the power-up self-tests described in Section 7.2. Upon successful completion of the power-up self-tests the TOE switches the peripheral group to channel 1 (indicating the selection of channel 1 with a solid LED).

The TOE does not implement a reset option.

FTA_CIN_EXT.1

When the user selects a different channel, the TOE removes power from the user authentication device. The TOE’s power circuit for the user authentication device contains 470 μF of capacitance, so the voltage will drop to 1.32v in 1 second when a low-power device is connected (i.e. a 100mA draw).

FTA_ATH_EXT.1

8 Terms and Definitions

Table 8: Technical Definitions

Abbreviations/ Acronyms	Description
Administrator	A person who administers (e.g. installs, configures, updates, maintains) a system of device(s) and connections.
Configurable Device Filtration	PSS function that qualifies (accepts or rejects) peripheral devices based on field configurable parameters.
Combiner	A PSS switch with video integration functionality.
Connected Computer	A computing device (platform) connected to the PSS. May be a personal computer, server, tablet or any other computing device with user interaction interfaces
Connection	Enables devices to interact through respective interfaces. It may consist of one or more physical (e.g. a cable) and/or logical (e.g. a protocol) components.
Device	An information technology product with which actors (persons or devices) interact.
Display	A Human Interface Device (HID), such as a monitor or touchscreen, which displays user data.
External Entity	An entity outside the TOE evaluated system, its connected computers and its connected peripheral devices.
Fixed Device Filtration	PSS function that qualifies (accepts or rejects) peripheral devices based on fixed parameters.
Human Interface Device	A device that allows for user input. For example, keyboard and mouse.
Interface	Enables interactions between actors.
Isolator	A PSS with a single connected computer.
Keyboard	A Human Interface Device (HID) such as a keyboard, keypad or other text entry device.
Non-Selected Computer	A connected computer not currently selected by the PSS user.
Peripheral	A device that exposes an actor’s interface to another actor.
Peripheral Group	An ordered set of peripherals.
Pointing Device	A Human Interface Device (HID), such as a mouse, track ball or touch screen (including multi-touch)
Selected Computer	A connected computer currently selected by the PSS user.
User	A person or device that interacts with devices and connections.
User Authentication Device	A peripheral device used to authenticate the identity of the user, such as a smart-card reader, biometric authentication device or proximity card reader.
Video Wall	Consists of multiple computer monitors, video projectors, or television sets tiled together contiguously or overlapped in order to form one large display.

Table 9: TOE Abbreviations and Acronyms

Abbreviations/ Acronyms	Description
AUX	DisplayPort Auxiliary Channel
CAC	Common Access Card
CDF	Configurable Device Filtration
CCTL	Common Criteria Test Lab
CDC	Communication Device Class
CLI	Command Line Interface
CODEC	Coder-Decoder

Table 9: TOE Abbreviations and Acronyms

Abbreviations/ Acronyms	Description
dBv	A measurement of voltages ratio – decibel volt
DC	Direct Current
DCU	Desktop Control Unit
DDC	Display Data Channel
DP	DisplayPort
DVI	Digital Visual Interface
EDID	Extended Display Identification Data
FDF	Fixed Device Filtration
FIPS	Federal Information Processing Standards
HD	High Definition
HDMI	High Definition Multimedia Interface
HEAC	HDMI Ethernet Audio Control
HID	Human Interface Device
KM	Keyboard, Mouse
KVM	Keyboard, Video and Mouse
LED	Light-Emitting Diode
MCCS	Monitor Control Command Set
MHL	Mobile High-Definition Link
MSC	Mass Storage Class
mV	millivolt
OSD	On-Screen Display
PC	Personal Computer
PS/2	6-pin Mini-DIN connector used for connecting some keyboards and mice to a PC compatible computer system.
PSS	Peripheral Sharing Switch
S/PDIF	Sony/Philips Digital Interface Format
SP	Special Publication
SPF	Shared Peripheral Functions
TMDS	Transition-Minimized Differential Signaling
UART	Universal Asynchronous Receiver / Transmitter
USB	Universal Serial Bus
USB Keep-Alive NAK transaction	USB 2.0 standard handshake PID (1010B) – Receiving device cannot accept data or transmitting device cannot send data.
V	Volt
VESA	Video Electronics Standards Association
VGA	Video Graphics Array

Table 10: CC Abbreviations and Acronyms

Abbreviations/ Acronyms	Description
CC	Common Criteria
CEM	Common Evaluation Methodology
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

Table 10: CC Abbreviations and Acronyms

Abbreviations/ Acronyms	Description
TSFI	TSF Interface
TSS	TOE summary specification - Documentation which provides evaluators with a description of the implementation of SFRs in the TOE.

9 References

Table 11: TOE Guidance Documentation

Reference	Description	Version	Date
[T1]	Administrative Guide	A1	October 19, 2017
[T2]	Administrator Guide for Secure Desktop Controller Unit (DCU)	A1	October 19, 2017

Table 12: TOE Evaluation Evidence

Reference	Description	Version	Date
[E1]	Isolation Documentation and Assessment	3.0	

Table 13: Common Criteria v3.1 References

Reference	Description	Version	Date
[C1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCMB-2012-09-001	V3.1 R4	September 2012
[C2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components CCMB-2012-09-002	V3.1 R4	September 2012
[C3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components CCMB-2012-09-003	V3.1 R4	September 2012
[C4]	Common Criteria for Information Technology Security Evaluation Evaluation Methodology CCMB-2012-09-004	V3.1 R4	September 2012

Table 14: Supporting Documentation

Reference	Description	Version	Date
[PSS]	Protection Profile for Peripheral Sharing Switch	3.0	February 13, 2015