# ADT WASP - ADTKVM2mDP

ST Version: 1.0.2

Date: 30 June 2026

Prepared for: Advanced Design Technology Pty Ltd

Prepared by:

TERON LABS

www.teronlabs.com

# Revision History

| Version | Date | Author(s) | Description of Change |
|---|---|---|---|
| 0.2 | 04-Sep-2024 | Teron Labs | Release with updated template and TSS updates. |
| 0.3 | 21-Jul-2025 | Teron Labs | Change to TOE scope. Updates resulting from EORs. |
| 0.5 | 04-Nov-2025 | Teron Labs | Updates resulting from EORs. |
| 0.6 | 05-Mar-2026 | Teron Labs | Updates resulting from EORs. |
| 0.7 | 11-May-2026 | Teron Labs | Updates resulting from EORs. |
| 1.0 | 12-May-2026 | Teron Labs | Updates resulting from EORs. |
| 1.0.1 | 23-May-2026 | Teron Labs | Minor wording update. |
| 1.0.2 | 30-Jun-2026 | Teron Labs | Minor reference update. |

# Contents


**1** Security Target Introduction ..... 4

1.1 Security Target Reference ..... 4

1.2 TOE Reference ..... 4

1.3 TOE Overview ..... 5

1.3.1 Intended Method of Use ..... 5

1.3.2 Major Security Features ..... 5

1.3.3 TOE Type ..... 5

1.4 TOE Description ..... 5

1.4.1 Logical Scope of the TOE ..... 5

1.4.2 TOE Documentation ..... 6

**2** Conformance Claims ..... 7

2.1 Statement of Conformance Claims ..... 7

2.2 Conformance Rationale ..... 8

2.2.1 TOE Type Consistency Rationale ..... 8

2.2.2 Security Problem Definition Consistency ..... 8

2.2.3 Security Objective Consistency ..... 8

2.2.4 Security Requirements Consistency ..... 8

2.3 Technical Decisions ..... 8

**3** Security Problem Description ..... 10

3.1 Threats ..... 10

3.2 Assumptions ..... 11

3.3 Organizational Security Policies ..... 11

**4** Security Objectives ..... 12

4.1 Security Objectives for the TOE ..... 12

4.2 Security Objectives for the Operational Environment ..... 14

4.3 Security Objectives Rationale ..... 14

**5** Security Requirements ..... 15

5.1 Extended Components Definition ..... 15

5.2 Notation and Conventions ..... 15

5.3 Security Functional Requirements Summary ..... 16

5.4 Class FDP: User Data Protection ..... 17

5.5 Class FPT: Protection of the TSF ..... 20

5.6 Class FTA: TOE Access ..... 21

**6** TOE Summary Specification ..... 22
6.1 Fulfillment of the Security Functional Requirements ..... 22
6.2 Fulfillment of the Security Assurance Requirements ..... 25
6.3 Security Requirements Rationale ..... 26
**7** Acronyms ..... 27
**8** References ..... 29
**9** Appendix A – Letter of Volatility ..... 30

# List of Tables

Table 1 TOE and ST Conformance Summary ..... 4
Table 2 Major Security Features ..... 5
Table 3 Technical Decisions applicable to the Base-PP [PP_PSD_V4.0] ..... 8
Table 4 Technical Decisions Applicable to [MOD_KM_V1.0] ..... 9
Table 5 Technical Decisions Applicable to [MOD_VI_V1.0] ..... 9
Table 6 SFR Summary ..... 16
Table 7 TSS Fulfilment ..... 22
Table 8 Security Assurance Components ..... 25

# 1 Security Target Introduction

This section is the Security Target introduction. It describes the Target of Evaluation (TOE) in a narrative way at three levels of abstraction: TOE Reference, TOE Overview and TOE Description. The objective is to assist the reader in understanding the TOE and in determining that the TOE is suitable for the intended use.

The target audience is the users and the potential users of the TOE wishing to gain a precise understanding of the TOE and the security features provided. The readers are expected to have a good understanding of computer security and are assumed to be proficient in Common Criteria terminology.

The Security Target (ST) Introduction commences with the statements of the Security Target Reference and the TOE Reference in Sections 1.1 and 1.2, respectively. The statement of the references is followed by the TOE Overview in Sect. 1.3. The TOE Description is given in Sect. 1.4.

The TOE and the ST claim conformance to Common Criteria CCv3.1 Revision 5. The TOE claims conformance to the Protection Profile and a Protection Profile Modules in accordance with a Protection Profile Configuration as identified in Table 1. The Terms given are used throughout the Security Target.

*Table 1 TOE and ST Conformance Summary*

| Term | Reference |
|---|---|
| Base-PP | Protection Profile for Peripheral Sharing Device, Version 4.0, 2019-07-19 (PP_PSD_V4.0) |
| PP-Modules | • PP-Module for Video/Display Devices, Version 1.0, 2019-07-19 (MOD_VI_V1.0)<br>• PP-Module for Keyboard/Mouse Devices, Version 1.0, 2019-07-19 (MOD_KM_V1.0) |
| PP-Configuration | PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, and Video/Display Devices, Version: 1.0, 2019-07-19 (CFG_PSD-KM-VI_V1.0) |

## 1.1 Security Target Reference

**ST Title** ADT WASP - ADTKVM2mDP

**ST Version** 1.0.2

**ST Date:** 30 June, 2026

## 1.2 TOE Reference

**TOE Identification** ADT WASP - ADTKVM2mDP

**TOE Developer** Advanced Design Technology Pty Ltd

**Evaluation Sponsor** Advanced Design Technology Pty Ltd

# 1.3 TOE Overview

## 1.3.1 Intended Method of Use

The TOE is a Peripheral Sharing Device (PSD) that allows users to share a keyboard and mouse with between two to four connected computers. The computers are connected to the TOE and share an external video device using mini-DisplayPort.

## 1.3.2 Major Security Features

The security features below are implemented by the TOE. Further details are provided in Section 1.4.

- Hardware Anti-Tampering
- Keyboard and Mouse Security
- Video Security

## 1.3.3 TOE Type

The TOE is a PSD that implements the security features required for exact conformance with the Base-PP and the PP-Modules.

# 1.4 TOE Description

ADT KVM, i.e. the TOE, is a KVM appliance designed to connect a single set of peripherals, including a mouse, keyboard and a maximum of two video displays to the TOE, supported via DisplayPort Multi-Stream Transport (MST) over a single physical port. The TOE's computer ports are connected to 2 separate computers. The user can then securely switch the connected console peripherals between the connected computers while preventing unintended or unauthorized data flows between computers. The TOE switches port based on the press and release of the port selection buttons on the TOE. The selected device is always identifiable by the lights associated with the applicable selection button.

The TOE's console ports support USB and DisplayPort ports. The TOE's computer ports support USB keyboard and mouse, and DisplayPort. The model designation for the TOE is ADTKVM2mDP.

The TOE hardware is made available to TOE consumers via courier delivery, hand delivery, or customer collection. The TOE firmware cannot be modified by the TOE user and is delivered in a CC configured state. The TOE user guidance is made available directly from the vendor once certified upon request.

## 1.4.1 Logical Scope of the TOE

The TOE implements the security functionality required by the Base-PP and the PP-Modules. The TOE implements the following security features to ensure there is no leakage of data between the connected computers. The major security features of the TOE are summarized in Table 2.

*Table 2 Major Security Features*

| Security Feature | Description |
|---|---|
| Hardware Anti-Tampering | • There are anti-tamper labels on the outside of the TOE. |

| | |
|---|---|
| | • All screws are hidden and require tools to access. |
| Keyboard and Mouse Security | • Non-Human Interface Devices (HID) data is blocked.<br>• Communication from computer to keyboard/mouse is blocked.<br>• One way data flow is enforced.<br>• The TOE emulates the behaviour of the keyboard/mouse to the connected console computers. |
| Video Security | • All video signals are processed by the TOE, with the AUX channel stripped away.<br>• The Extended Display Identification Data (EDID) is emulated by the TOE for the connected console computers as read only.<br>• The access to the monitors EDID is blocked by the TOE<br>• The DisplayPort data packets are stripped back to raw data frames while in the TOE. |

No assurance is extended to peripherals or monitors when they are used outside the bounds of the TOE.

### 1.4.2 TOE Documentation

The TOE includes the following documentation:

[TOE Guidance] – Guidance Document, KVM Project, ADT WASP - ADTKVM2mDP, Version 2.1, 26 June 2026

# 2 Conformance Claims

This section states the Conformance Claims for the ST and the TOE. This includes a statement of the Conformance Claims, a statement of the Conformance Claim Rationale, and the Identification of the Technical Decisions applicable to the TOE.

## 2.1 Statement of Conformance Claims

The ST and the TOE claim conformance to Common Criteria Version 3.1 Revision 5, Part 1 through to Part 3 identified in the following:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, April 2017, Version 3.1 Revision 5, CCMB-2017-04-001
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-002
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-003

The ST claims CC Part 2 conformance as CC Part 2 Extended.

The ST claims CC Part 3 conformance as CC Part 3 Conformant.

The ST claims conformance to the following Protection Profile, and the Protection Profile Modules:

- Protection Profile for Peripheral Sharing Device v4.0, Date: 19-July-2019 (PP_PSD_V4.0)
- PP-Module for Keyboard/Mouse Devices, Version 1.0, Date: 19-July-2019 (MOD_KM_V1.0)
- PP-Module for Video/Display Devices, Version 1.0, Date: 19-July-2019 (MOD_VI_V1.0)

Conformance to the Base-PP and the PP-Module is claimed in accordance with the PP-Configuration:

- PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, and Video/Display Devices, Version: 1.0, 2019-07-19 (CFG_PSD-KM-VI_V1.0)

The ST claims no conformance to any Evaluation Assurance Level or any other security assurance requirement package. Security assurance requirements applicable to the TOE are those drawn from the Base-PP as required by Sect. 2.2 of CFG_PSD-KM-VI_V1.0.

The ST claims conformance to the Protection Profile for Peripheral Sharing Device v4.0, Date: 19-July-2019 (PP_PSD_V4.0) as PP-conformant.

The ST claims conformance to the PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, and Video/Display Devices, Version: 1.0, 2019-07-19 (CFG_PSD-KM-VI_V1.0) as PP-configuration-conformant.

The ST claims exact conformance to the Base-PP, exact conformance to each PP-Module, and exact conformance to the PP-configuration[1].

[1] Exact conformance is defined in *CC and CEM addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs, CCDB-013-v2.0 Final, 2021-Sep-30.*

## 2.2 Conformance Rationale

### 2.2.1 TOE Type Consistency Rationale

The TOE is a KVM switch. It implements a set of security features required for exact conformance with the Base-PP and with the PP-Modules. The PP and the PP-Modules are used in accordance with the PP-Configuration. These are exactly the PP, the PP-Module, and the PP-configuration claimed in Sect. 2.1. The PP and the PP-Modules are exactly as identified in Sect. 1.3 of the PP-Configuration. This ensures that the TOE Type is consistent with the TOE Type in the Base-PP, PP-Modules, and PP-Configuration.

### 2.2.2 Security Problem Definition Consistency

The statement of the Security Problem Definition in this ST is reproduced exactly from the Base-PP and from the claimed PP-Modules. The resulting Security Problem Definition is a union of the Security Problem Definition of the Base-PP and the PP-Modules. There are no additional Security Problem Definition elements included in the statement of the Security Problem Definition. This ensures that the statement of the Security Problem Definition is consistent with the PP-Configuration.

### 2.2.3 Security Objective Consistency

The statement of the Security Objectives in this ST is reproduced exactly from the Base-PP and the PP-Modules. The resulting Security Objectives statement is a union of the Security Objectives of the Base-PP and the PP-Modules. There are no additional Security Objectives included in the statement of the Security Objectives. This ensures that the statement of the Security Objectives is consistent with the PP-Configuration.

### 2.2.4 Security Requirements Consistency

The security functional requirements are drawn exactly from the Base-PP and the PP-Modules. The statement of the security functional requirements includes all mandatory security requirements and those selection-based security functional requirements applicable to the TOE. As such, the security functional requirements are consistently drawn from the Base-PP and the PP-Modules, and the ST ensures the consistency of the security functional requirements.

The security assurance requirements are drawn from the Base-PP only. This is consistent with Sect. 2.2 of the PP-Configuration. This ensures the consistency of the security assurance requirements.

## 2.3 Technical Decisions

The Technical Decisions (TD) applicable to the Base-PP are given in. That is followed by the identification of each TD applicable to the PP-Modules For each TD, the applicability to the ST is stated. For each TD which is not applicable, a brief justification for the exclusion is given.

*Table 3 Technical Decisions applicable to the Base-PP [PP_PSD_V4.0]*

| TD | Description | Applicable | Exclusion Rationale (if applicable) |
|---|---|---|---|
| TD0844 | Addition of Assurance Package for Flaw Remediation V1.0 Conformance Claim | No | The Assurance package Flaw Remediation is not claimed. |
| TD0804 | Clarification regarding Extenders in PSD Evaluations | Yes | |

| | | | |
|---|---|---|---|
| TD0583 | FPT_PHP.3 modified for PSD remote controllers | Yes | |
| TD0518 | Typographical error in Dependency Table | Yes | |

*Table 4 Technical Decisions Applicable to [MOD_KM_V1.0]*

| TD | Description | Applicable | Exclusion Rationale (if applicable) |
|---|---|---|---|
| TD0959 | Correction to Test 4 Step 3 of FDP_APC_EXT.1 | Yes | |
| TD0593 | Equivalency Arguments for PSD | Yes | |
| TD0507 | Clarification on USB plug type | Yes | |

*Table 5 Technical Decisions Applicable to [MOD_VI_V1.0]*

| TD | Description | Applicable | Exclusion Rationale (if applicable) |
|---|---|---|---|
| TD0942 | Updated EDID Read Requirements | Yes | |
| TD0842 | Alternate Conversion Option for FDP_IPC_EXT.1 | Yes | |
| TD0686 | DisplayPort CEC Testing | Yes | |
| TD0681 | PSD purging of EDID data upon disconnect | Yes | |
| TD0593 | Equivalency Arguments for PSD | Yes | |
| TD0584 | Update to FDP APC_EXT.1 Video Tests | Yes | |
| TD0539 | Incorrect selection trigger in FTA_CIN_EXT.1 in MOD_VI_V1.0 | Yes | |
| TD0514 | Correction to MOD_VI FDP_APC_EXT.1 Test 3 Step 6 | Yes | |
| TD0506 | Missing Steps to disconnect and reconnect display | Yes | |

# 3 Security Problem Description

The security problem description for the TOE which includes the threats, assumptions and organizational security policies relevant to the TOE are listed here. They are taken from [PP_PSD_V4.0], [MOD_KM_V1.0], and [MOD_VI_V1.0] and reproduced here.

## 3.1 Threats

The threats for the PSD are listed in the sections below. The description of each threat is then followed by a rationale describing how it is addressed by the SFRs in the following chapters.

### 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.

## 3.2 Assumptions

This section describes the assumptions made in identification of the threats and security requirements for PSD. The PSD is not expected to provide assurance in any of these areas, and as a result, requirements are not included to mitigate the threats associated.

A.NO_TEMPEST Computers and peripheral devices connected to the PSD are not TEMPEST approved. The TSF may or may not isolate the ground of the keyboard and mouse computer interfaces (the USB ground). The Operational Environment is assumed not to support TEMPEST red-black ground isolation.

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.

A.NO_SPECIAL_ANALOG_CAPABILITIES 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, or analog video capture function.

## 3.3 Organizational Security Policies

This Protection Profile does not define any organizational security policies.

# 4 Security Objectives

The security objectives for the TOE and for the environment are taken from [PP_PSD_V4.0], [MOD_KM_V1.0], and [MOD_VI_V1.0] and reproduced here.

## 4.1 Security Objectives for the TOE

O.COMPUTER_INTERFACE_ISOLATION 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 the TOE is powered.

Addressed by: FDP_APC_EXT.1

O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED The PSD shall not allow data to transmit a PSD-Computer interface while the PSD is unpowered.

Addressed by: FDP_APC_EXT.1

O.USER_DATA_ISOLATION 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: FDP_APC_EXT.1

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: FDP_RIP_EXT.1, FDP_RIP_EXT.2 (optional)

O.NO_OTHER_EXTERNAL_INTERFACES The PSD shall not have any external interfaces other than those implemented by the TSF.

Addressed by: 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: FDP_SWI_EXT.1, FDP_SWI_EXT.2 (selection-based)

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 button, 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: FAU_GEN.1 (optional), FDP_SWI_EXT.1, FDP_SWI_EXT.2 (selection-based), FIA_UAU.2 (optional), FIA_UID.2 (optional), FMT_MOF.1 (optional), FMT_SMF.1 (optional), FMT_SMR.1 (optional), FPT_STM.1 (optional), FTA_CIN_EXT.1 (selection-based)

O.PERIPHERAL_PORTS_ISOLATION The PSD shall ensure that data does not flow between peripheral devices connected to different PSD interfaces.

Addressed by: FDP_APC_EXT.1

O.REJECT_UNAUTHORIZED_PERIPHERAL The PSD shall reject unauthorized peripheral device types and protocols.

Addressed by: FDP_PDC_EXT.1

O.REJECT_UNAUTHORIZED_ENDPOINTS The PSD shall reject unauthorized peripheral devices connected via a Universal Serial Bus (USB) hub.

Addressed by: FDP_PDC_EXT.1

O.NO_TOE_ACCESS The PSD firmware, software, and memory shall not be accessible via its external ports.

Addressed by: FPT_NTA_EXT.1

O.TAMPER_EVIDENT_LABEL 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 labelled 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: 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: FPT_PHP.1, FPT_PHP.3 (optional)

O.SELF_TEST The PSD shall perform self-tests following power up or powered reset.

Addressed by: FPT_TST.1

O.SELF_TEST_FAIL_TOE_DISABLE The PSD shall enter a secure state upon detection of a critical failure.

Addressed by: 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: FPT_TST_EXT.1

O.PROTECTED_EDID The TOE shall read the connected display Extended Display Identification Data (EDID) once during the TOE power up or reboot sequence and prevent any EDID channel write transactions that connected computers initiate.

Addressed by: FDP_PDC_EXT.2/VI, FDP_SPR_EXT.1/DP (selection-based), FDP_SPR_EXT.1/DVI-D (selection-based), FDP_SPR_EXT.1/DVI-I (selection-based), FDP_SPR_EXT.1/HDMI (selection-based), FDP_SPR_EXT.1/USB (selection-based), FDP_SPR_EXT.1/VGA (selection-based)

O.UNIDIRECTIONAL_VIDEO The TOE shall enforce unidirectional video data flow from the connected computer video interface to the display interface only.

Addressed by: FDP_UDF_EXT.1/VI

O.EMULATED_INPUT The TOE shall emulate the keyboard and/or mouse functions from the TOE to the connected computer.

Addressed by: FDP_PDC_EXT.2/KM, FDP_PDC_EXT.3/KM

O.UNIDIRECTIONAL_INPUT The TOE shall enforce unidirectional keyboard and/or mouse device's data flow from the peripheral device to only the selected computer.

Addressed by: FDP_UDF_EXT.1/KM

## 4.2 Security Objectives for the Operational Environment

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.

OE.NO_SPECIAL_ANALOG_CAPABILITIES The operational environment will not have special analog data collection cards or peripherals such as analog to digital interface, high performance audio interface, or a component with digital signal processing or analog video capture functions.

## 4.3 Security Objectives Rationale

Security objectives for the TOE and the operational environment are identical to those specified in Sect. 4.3 of [PP_PSD_v4.0], [MOD_KM_V1.0], and [MOD_VI_V1.0]. The rationales are, therefore, also identical and are not reproduced here.

# 5 Security Requirements

This section states the security requirements applicable to the TOE. The statement commences with the extended components definition in Sect. 5.1. The statement of the extended components is followed by the statement of the notations and conventions used in the expression of the security requirements. The security functional requirements are summarized in Sect. 5.3 and stated in the subsequent subsections on a per functional class basis. The security assurance requirements are only drawn from the Base-PP and are given in Sect. 6.2. The security requirements rationale is given in Sect. 6.3.

This section states the Security Functional Requirements and Security Assurance Requirements for the TOE.

## 5.1 Extended Components Definition

The ST references several extended components. Each one is taken verbatim from the Base-PP or the PP-Modules. Only the operations allowed in the statement of the extended components are implemented in the ST. There are no additional or modified extended components included in the ST. Therefore, the statement of the extended components is exactly as in the Base-PP and the PP-Modules. They are not repeated here.

## 5.2 Notation and Conventions

This ST follows the specific conventions in the completion of the operations on the Security Functional Requirements. The following conventions are followed to indicate the operations:

- Unaltered SFRs are stated in accordance with [CCPart2] or the extended component definition;
- Refinement is indicated with **bold text** and ~~strikethroughs~~;
- Selection is indicated with *italicized* text;
- Assignment is indicated with *italicized and underlined* text;
- Iteration is indicated by adding a string starting with "/" (e.g. "FDP_PDC_EXT.2/AO"); and
- Extended SFRs are identified by having a label "_EXT" at the end of the SFR name as defined in the extended components definition (e.g. FDP_APC_EXT.1).

Any conventions deviating from the above in [PP_PSD_V4.0] shall also be used in the ST.

## 5.3 Security Functional Requirements Summary

The Security Functional Requirements applicable to the TOE as drawn from different sources are summarized in Table 6. On those occasions where a PP-Module refines the statement of a security functional component of a Base-PP, the component is listed under the PP-Module with an indication of the statement in the PP-Module being refined from that in the Base-PP. When a PP-Module makes an optional or selection-based component of a Base-PP mandatory, this is also indicated.

*Table 6 SFR Summary*

| Security Functional Class | Security Functional Components Drawn from the Base-PP |
|---|---|
| FDP: User Data Protection | FDP_CDS_EXT.1.1 External Displays Supported<br>FDP_IPC_EXT.1 Internal Protocol Conversion<br>FDP_PDC_EXT.1 Peripheral Device Connection<br>FDP_RIP_EXT.1 Residual Information Protection<br>FDP_RIP_EXT.2 Purge of Residual Information<br>FDP_SWI_EXT.1 PSD Switching<br>FDP_SWI_EXT.2 PSD Switching Methods |
| FPT: Protection of the TSF | FPT_FLS_EXT.1 Failure with Preservation of Secure State<br>FPT_NTA_EXT.1 No Access to TOE<br>FPT_PHP.1 Passive Detection of Physical Attack<br>FPT_PHP.3 Resistance to Physical Attack<br>FPT_TST.1 TSF Testing<br>FPT_TST_EXT.1 TSF Testing |
| FTA: TOE Access | FTA_CIN_EXT.1 Continuous Indications |
| Security Functional Class | Security Functional Components Drawn from [MOD_KM_V1.0] |
| FDP: User Data Protection | FDP_APC_EXT.1/KM Active PSD Connections<br>FDP_FIL_EXT.1/KM Device Filtering<br>FDP_PDC_EXT.2/KM Peripheral Device Connection<br>FDP_PDC_EXT.3/KM Authorized Connection Protocols<br>FDP_UDF_EXT.1/KM Unidirectional Data Flow<br>FDP_RIP.1/KM Residual Information Protection<br>FDP_SWI_EXT.3 Tied Switching<br>FDP_RDR_EXT.1 Re-Enumeration Device Rejection |

| Security Functional Class | Security Functional Components Drawn from [MOD_VI_V1.0] |
|---|---|
| FDP: User Data Protection | FDP_APC_EXT.1/VI Active PSD Connections<br>FDP_UDF_EXT.1/VI Unidirectional Data Flow<br>FDP_SPR_EXT.1/DP Sub-Protocol Rules<br>FDP_PDC_EXT.2/VI Peripheral Device Connection<br>FDP_PDC_EXT.3/VI Authorized Connection Protocols |
| FTA: TOE Access | FTA_CIN_EXT.1/VI Continuous Indications |

## 5.4 Class FDP: User Data Protection

FDP_APC_EXT.1/KM Active PSD Connections (Keyboard/Mouse)

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

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

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

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

FDP_APC_EXT.1/VI Active PSD Connections (Video Output)

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

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

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

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

FDP_CDS_EXT.1 Connected Displays Supported

FDP_CDS_EXT.1.1 The TSF shall support [ *multiple connected displays*] at a time.

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

FDP_FIL_EXT.1.1/KM The TSF shall have [*fixed*] device filtering for [*keyboard*, *mouse*] interfaces.

FDP_FIL_EXT.1.2/KM The TSF shall consider all [*PSD KM*] blacklisted devices as unauthorized devices for [*keyboard*, *mouse*] interfaces in peripheral device connections.

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

### FDP_IPC_EXT.1 Internal Protocol Conversion

FDP_IPC_EXT.1.1 The TSF shall convert the [*DisplayPort*] protocol at the [*DisplayPort peripheral display interface(s)*] into the [*YCbCr*] protocol within the TOE.

FDP_IPC_EXT.1.2 The TSF shall output the [*YCbCr*] protocol from inside the TOE to [*computer video interface*] as [*[DisplayPort] protocol*].

### 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.

### FDP_PDC_EXT.2/KM Peripheral Device Connection (Keyboard/Mouse)

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

- *authorized devices as defined in the PP-Module for Video/Display Devices*,
- *no other device*

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

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

- *authorized devices as defined in the PP-Module for Video/Display Devices*,
- *no other device*

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

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

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

- *authorized devices as defined in the PP-Module for Keyboard/Mouse Devices*,
- *no other device*

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

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

- *authorized devices as defined in the PP-Module for Keyboard/Mouse Devices*
- *no other device*

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

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

FDP_PDC_EXT.3.1/KM The TSF shall have interfaces for the [*USB (keyboard)*, *USB (mouse*] protocols.

FDP_PDC_EXT.3.2/KM The TSF shall apply the following rules to the supported protocols: [*the TSF shall emulate any keyboard or mouse device functions from the TOE to the connected computer*].

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

FDP_PDC_EXT.3.1/VI The TSF shall have interfaces for the [*DisplayPort*] protocols.

FDP_PDC_EXT.3.2/VI The TSF shall apply the following rules to the supported protocols: [*the TSF shall read the connected display EDID information once during power-on or reboot* [*automatically*]].

FDP_RDR_EXT.1 Re-Enumeration Device Rejection

FDP_RDR_EXT.1.1 The TSF shall reject any device that attempts to enumerate again as a different unauthorized device.

FDP_RIP.1/KM Residual Information Protection (Keyboard Data)

FDP_RIP.1.1/KM The TSF shall ensure that any keyboard data in volatile memory is purged upon switching computers.

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.

FDP_RIP_EXT.2 Purge of Residual Information

FDP_RIP_EXT.2.1 The TOE shall have a purge memory or restore factory defaults function accessible to the administrator to delete all TOE stored configuration and settings except for logging.

FDP_SPR_EXT.1/DP Sub-Protocol Rules (DisplayPort Protocol)

FDP_SPR_EXT.1.1 The TSF shall apply the following rules for the [DisplayPort] protocol:

- Block the following video/display sub-protocols:
  - [*CEC*,
  - *EDID from computer to display*,
  - *HDCP*,
  - *MCCS*]
- Allow the following video/display sub-protocols:
  - [*EDID from display to computer*,
  - *HPD from display to computer*,
  - *Link Training*]

### 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*]

### 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*].

### FDP_SWI_EXT.3 Tied Switching

**FDP_SWI_EXT.3.1** The TSF shall ensure that [*connected keyboard and mouse peripheral devices*] are always switched together to the same connected computer.

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

**FDP_UDF_EXT.1.1/KM** The TSF shall ensure [*keyboard, mouse*] data transits the TOE unidirectionally from the [ *TOE [keyboard, mouse]*] peripheral interface(s) to the [ *TOE [keyboard, mouse]*] interface.

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

**FDP_UDF_EXT.1.1/VI** The TSF shall ensure [*video*] data transits the TOE unidirectionally from the [ *TOE computer video*] interface(s) to the [*TOE peripheral device display]*] interface.

## 5.5 Class FPT: Protection of the TSF

### 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 [*failure of the anti-tamper function, no other failures*].

### 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: [*the EDID memory of Video TOEs may be accessible from connected computers*].

### 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.

### FPT_PHP.3 Resistance to Physical Attack

FPT_PHP.3.1 [2]The TSF shall resist [*a physical attack for the purpose of gaining access to the internal components, to damage the anti-tamper battery, to drain or exhaust the anti-tamper battery*] to the [*TOE enclosure and any remote controllers*] by the attacked component becoming permanently disabled.

### 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 [active anti-tamper functionality, 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*].

### 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.

## 5.6 Class FTA: TOE Access

### 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 button, a blue or a salmon-coloured light*].

FTA_CIN_EXT.1.3 The TSF shall ensure that while the TOE is powered the current switching status is reflected by [*multiple indicators which never display conflicting information*]

### FTA_CIN_EXT.1/VI Continuous Indications

FTA_CIN_EXT.1.2/VI 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** [*[border around video frame]*].

[2] Modified by TD0583.

# 6 TOE Summary Specification

The TOE Summary Specification includes the description of how the TOE fulfills the security functional requirements, and how the developer and the evaluator fulfill the security assurance requirements. Each is described in this section. Additional details on the cryptographic algorithms and protocols implemented in the TOE are also given.

## 6.1 Fulfillment of the Security Functional Requirements

The fulfilment of the Security Functional Components by the TOE is given in Table 7. Each Security Functional Component applicable to the TOE is listed and the fulfilment of that component described.

*Table 7 TSS Fulfilment*

| Security Functional Component | Fulfilment |
|---|---|
| FDP_APC_EXT.1/KM<br>FDP_APC_EXT.1/VI | The only failure state defined is the removal or modification of the encrypted FPGA binary image stored in shared program memory. If the FPGA image fails its integrity test, the TOE will be non-functional, with red lights showing around the logo and all source-select buttons.<br>The integrity test will detect any change (including a single bit) to the FPGA image. Further details will be contained in the [Isolation Document]. |
| FDP_CDS_EXT.1 | The maximum number of monitors supported is two (2), via Multi Stream Transport (MST). |
| FDP_FIL_EXT.1/KM | The PSD has fixed device filtering. |
| FDP_IPC_EXT.1 | The DisplayPort data consists of two streams, the Main Link (ML) differential pairs carrying video data (including Main Stream Attribute) and an AUX channel which carries auxiliary data, including the monitor EDID information.<br>The DisplayPort data is presented to the FPGA as differential pairs and are converted to a parallel binary stream by the transceivers, using an internal FPGA video image binary format (defined by the FPGA vendor within their Display Port FPGA Intellectual Property (IP) block). The Main Link (ML) Lanes (up to 4) are strictly unidirectional (from source to monitor) and are switched within the FPGA from amongst the different sources. At the output, the binary stream is converted back to differential pairs by the transceivers within the FPGA. Main Stream Attribute (MSA) metadata is extracted from the ML, processed in the FPGA and presented to the monitor/s. MSA from one PC cannot “spill over” to other sources as it bypasses the (virtual) processor/s and is injected directly into the ML stream.<br>The AUX channel is isolated and processed separately. Only the EDID message from the monitor is allowed to pass the data diode. This is stored in one-time-write memory (resettable via a power cycle) and presented to the connected PC. All other messages on the AUX channel are ignored by the TSS. No AUX data is directly passed from PC to monitor. |

| | |
|---|---|
| FDP_PDC_EXT.1 | Compatible devices for each port:<br>• USB ports (Type A, qty 3): USB HID devices (mouse & keyboard device classes only)<br>• Monitor port (miniDP, qty 1): DP monitor devices & HDMI / DVI monitors connected via an external (passive) (DP++) adaptor<br>• Connected PC ports (miniDP, qty 1 and Type-C, qty 1, per source): DP source devices (video cards, etc) and USB upstream devices. The Type C ports only connect the power and USB2 D+ and D- lines; the 4 SuperSpeed (USB3+) differential pairs are not connected.<br>There are no further external connectors and there are no wireless interfaces.<br>The KVM will enumerate all valid USB keyboard and mouse devices (including multiples). If a combination device (such as a keyboard with integrated microphone) the KVM will only enumerate the valid devices and ignore the unauthorised devices, providing the user feedback in the form of a flashing red logo on the KVM. USB Hubs are not supported by the TOE.<br>The TOE enumerates multiple keyboards and mouses, like normal computer behaviour, due to the use case of a user using a mini keyboard with a separately attached numeric keypad and / or specialised, alternate mouse for particular tasks (e.g. CAD). |
| FDP_PDC_EXT.3/KM | The KVM presents emulated keyboard and mouse devices, with unique device IDs.<br>Keyboard strokes and mouse button / movement events are stripped of their headers, leaving only the event (e.g. keypress, movement vector, etc.) at the USB side and recreated and presented to the connected source.<br>This path is strictly one way, from the USB HID to PC. |
| FDP_RDR_EXT.1 | The TOE checks each connected device on connection and only enumerates valid USB devices (USB HID class, keyboard and mouse device classes). |
| FDP_RIP.1/KM | User data buffers are contained within the FPGA (within a volatile memory block). These data buffers are cleared when a user selects a new source by erasing the buffer.<br>The Caps, Num and Scroll lock key state, particular to a connected PC are not buffered, rather the status is stored as the state of discrete I/O flags that are presented to the USB Host Processor (Figure on Page 13 of the [Isolation Document]) by each PC Processor. |
| FDP_RIP_EXT.1 | Details are contained in Appendix A – Letter of Volatility. |
| FDP_RIP_EXT.2 | “Memory purge” is not relevant to the implementation of the TOE. “Restore factory defaults” is conducted on power-cycle; there is no volatile memory that is external to the FPGA.<br>On power cycle, the FPGA is re-imaged, erasing any stored data, hence no information is carried over from the previous state. |
| FDP_SPR_EXT.1/DP | The Display Port AUX channel is isolated and processed separately. The EDID exchange is isolated into two separate and independent isolated transactions. The TOE initially requests the EDID from the monitor, once, at startup. This |

| | |
|---|---|
| | cached EDID is then used to respond to future EDID requests from the PCs; all other messages on the AUX channel are ignored by the TOE. No AUX data is directly passed from PC to monitor.<br><br>Details on how any sub-protocols are handled can be found in pages 12 and 13 of the [Isolation Document]. |
| FDP_SWI_EXT.1 | The TOE only switches sources via the user pressing the individual source button on top of the unit. There is no remote control, nor the ability for any connected device to automatically switch sources (e.g. via keypress). |
| FDP_SWI_EXT.2 | Source switching is initiated by user button press. On receipt, the TOE clears the USB information buffer, flushes the DP buffer and then switches the DP link and USB buffers. |
| FDP_SWI_EXT.3 | The TOE only connects the keyboard and mouse to the selected source. TOE maintains USB connections with unselected sources, but no data is presented to them.<br><br>The FPGA logic implementation prevents a keyboard or mouse event being sent to an unconnected source. |
| FDP_UDF_EXT.1/KM | In the USB standard, the Caps Lock, Num Lock, and Scroll Lock ("CNS") indicators are stored by the connected source (PC) and USB messages indicate to the connected computer that a CNS key has been selected on the keyboard.<br><br>The KVM does not forward any CNS indicators to an attached keyboard. CNS indicators are only sent from the peripheral, through the TOE and to the connected computer. The communication for this indicator type is uni-directional. There are no displays on the TOE to indicate the CNS status. |
| FPT_FLS_EXT.1 | Addressed by FPT_TST.1 |
| FPT_NTA_EXT.1 | Details are provided in the [Isolation Document]. |
| FPT_PHP.1 | The TOE has the following protection mechanisms:<br><br>• Wafer seals to indicate the case being opened, and,<br>• Self-protection mechanisms to indicate opening of the case, making the KVM inoperable.<br><br>In addition, the TOE has a Kensington lock slot to prevent unauthorised relocation or removal; the opening of this slot does not allow access to the interior of the TOE. Likewise, the case prevents objects being inserted around the external connectors to access the main circuit board. |
| FPT_PHP.3 | If a tamper event is detected, the TOE shows red lights on the logo and all buttons (the "failure" state).<br><br>There is no test required of the user interface; the design of the buttons prevents jamming (capacitive touch sensors). LED failures cannot be detected but as multiple LEDs are used for each indicator, multiple failures can be tolerated before the indicator fails.<br><br>The anti-tamper mechanism is purely passive and will activate should the battery backup fail (or drop beneath a set voltage). This requires users to return the device to the factory for battery replacement. |

| | |
|---|---|
| | Upon failure, the TOE does NOT shutdown; it remains in an inoperative state showing the failure indicator (red logo and source LEDs). |
| FPT_TST.1 | The TOE performs several self-tests on device power-up. These are addressed in paragraph 30 of the [Isolation Document]. |
| FPT_TST_EXT.1 | In the case of a self-test failure, the KVM will show a purple logo and alternating blue and red lights on each button (e.g. for a 2 port, button 1 will be blue, the other red; for 4 port, buttons 1 and 3 will be blue, 2 and 4 red). A power cycle is required to clear this fault. The KVM does not process any user data until the device is in the On state. |
| FTA_CIN_EXT.1<br>FTA_CIN_EXT.1/VI | For the TOE, power up and reset events are identical and follow the state diagram shown in Figure 1 in the [Isolation Document]. During startup, no connected computer interfaces are active; these only become active in the "On" state.<br>On startup, the TOE defaults to Source 1, and connects the keyboard and mouse to this source, and the source DP to the connected monitor/s. Button 1 (reflecting Source 1) will display a bright coloured ring around the button; all other buttons with connected sources will show their individual colour (per below) but dim. In all cases, the logo will be white. If no source is detected on a particular port, the corresponding LED will not be enabled. |

## 6.2 Fulfillment of the Security Assurance Requirements

The Security Assurance Requirements applicable to the TOE do not constitute any Evaluation Assurance Level (EAL) or other assurance package. Instead, they are taken from [PP_PSD_V4.0], [MOD_KM_V1.0], and [MOD_VI_V1.0] and the associated Supporting Documents. The Security Assurance Requirements applicable to the TOE are summarized in Table 8 Security Assurance Components.

*Table 8 Security Assurance Components*

| ASSURANCE CLASS | ASSURANCE COMPONENT |
|---|---|
| Security Target (ASE) | Conformance claims (ASE_CCL.1) |
| | Extended components definition (ASE_ECD.1) |
| | ST introduction (ASE_INT.1) |
| | Security objectives (ASE_OBJ.2) |
| | Derived security requirements (ASE_REQ.2) |
| | Security Problem Definition (ASE_SPD.1) |
| | TOE summary specification (ASE_TSS.1) |
| Development (ADV) | Basic functional specification (ADV_FSP.1) |

| | |
|---|---|
| Guidance Documents (AGD) | Operational user guidance (AGD_OPE.1) |
| | Preparative procedures (AGD_PRE.1) |
| Life Cycle Support (ALC) | Labelling of the TOE (ALC_CMC.1) |
| | TOE CM coverage (ALC_CMS.1) |
| Tests (ATE) | Independent testing – conformance (ATE_IND.1) |
| Vulnerability Assessment (AVA) | Vulnerability survey (AVA_VAN.1) |

## 6.3 Security Requirements Rationale

The Security Functional Requirements are drawn from the Base-PP and PP-Module and not from any other source. The ST claims exact conformance to the Base-PP and to the PP-Module. The Security Functional Requirements include each mandatory requirement and each applicable optional and selection-based requirement. Only the operations allowed in the Base-PP and the PP-Module are implemented. Therefore, the Security Functional Rationales of the Base-PP and the PP-Module are directly applicable to the ST as well. They are not repeated here.

The Security Assurance Requirements are drawn from the Base-PP only as required by the PP-Configuration. None. are added or removed. Therefore, the Security Assurance Requirements Rationale of the Base-PP is directly applicable to the ST as well. It is not repeated here.

# 7 Acronyms

| | |
|---|---|
| **AO** | Audio Output |
| **ASCII** | American Standard Code for Information Interchange |
| **AUX** | Auxiliary |
| **BIOS** | Basic Input Output System |
| **CC** | Common Criteria |
| **CCEVS** | Common Criteria Evaluation and Validation Scheme |
| **CEM** | Common Evaluation Methodology |
| **DP** | Display Port |
| **FIPS** | Federal Information Processing Standard |
| **FIPS PUB** | FIPS Publication |
| **FPGA** | Field Programmable Gate Arrays |
| **HDMI** | High-Definition Multimedia Interface |
| **HID** | Human Interface Device |
| **IEEE** | Institute of Electrical and Electronics Engineers |
| **IP** | Internet Protocol |
| **ISO** | International Organization for Standardization |
| **IT** | Information Technology |
| **KM** | Keyboard/Mouse |
| **KVM** | Kernel-based Virtual Machine |
| **LAN** | Local Area Network |
| **LED** | Light Emitting Diode |
| **MAC** | Media Access Control<br>or: Message Authentication Code |
| **NIAP** | National Information Assurance Partnership |
| **NIST** | National Institute of Standards and Technology |
| **NTP** | Network Time Protocol |
| **OID** | Object Identity |
| **OS** | Operating System |
| **OSP** | Organizational Security Policy |
| **P2P** | Point-to-Point |
| **PSD** | Peripheral Sharing Device |

| | |
|---|---|
| **QA** | Quality Assurance |
| **RFC** | Request For Comments |
| **SD** | Supporting Document |
| **SAR** | Security Assurance Requirement |
| **SFR** | Security Functional Requirement |
| **SNMP** | Simple Network Management Protocol |
| **SSD** | Solid State Drive |
| **TSF** | TOE Security Function |
| **USB** | Universal Serial Bus |
| **VGA** | Video Graphics Array |
| **VI** | Video/Display |
| **VPN** | Virtual Private Network |

# 8 References

| | |
|---|---|
| **CC** | *CC v3.1. Release 5*<br>• Part 1: Introduction and general model<br>• Part 2: Security functional requirements<br>• Part 3: Security assurance requirements<br>• CEM |
| **NIAP Policy Letter #5** | Applicability and Relationship of NIST Cryptographic Algorithm Validation Program (CAVP) and Cryptographic Module Validation Program (CMVP) to NIAP's Common Criteria Evaluation and Validation Scheme (CCEVS)<br>• Addendum #1 – Frequently Asked Questions for NIAP Policy #5<br>• Addendum #2 – CAVP Mapping, Version 2.0 |
| **PP/cPP** | Protection Profile for Peripheral Sharing Device, Version 4.0, 2019-07-19 (PP_PSD_V4.0) |
| **PP Module (As needed)** | PP-Module for Video/Display Devices, Version 1.0, 2019-07-19 (MOD_VI_V1.0)<br>PP-Module for Keyboard/Mouse Devices, Version 1.0, 2019-07-19 (MOD_KM_V1.0) |

# 9 Appendix A – Letter of Volatility

### Components Containing Non-Volatile Memory

The components within the Target of Evaluation (TOE) containing non-volatile memory are listed below:

Description: Clock Generator 6-output
Manufacturer: Skyworks
Part Number: SI5332B-D-GM1
Memory technology: simple register values and basic configuration data configured via I2C
Memory size: trivial

Description: Flash SPI FLASH NOR SLC 64MX4 TBGA
Manufacturer: Micron
Part Number: MT25QU256ABA8E12-0AAT
Memory technology: Flash Memory
Memory size: 32MB (256Mb)

### Data and Data Types Stored by TOE

The clock generator data is made up of basic configuration settings for output clock frequency and I2C address information. The Flash data is made up of an encrypted FPGA image and upon power up of the TOE is loaded to volatile memory within an FPGA and then decrypted.

### Statement on the Storage of User Data

User data is not stored on the TOE non-volatile memory or storage, which includes the clock generator and flash.

### Use of Independent Power Sources

The clock generator and flash cannot be independently powered outside of the designated user power source (USB and/or DP).

### Effects of Restoration to Factory Default

Restoration to factory default setting occurs when power cycling the TOE. Upon restoration to factory default setting, the clock generator retains the output clock frequency settings and I2C address information, and the flash retains the encrypted FPGA image. The FPGA image previously loaded and decrypted onto the FPGA is lost but is re-retrieved from flash and decrypted again automatically within the FPGA.