Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

ADT WASP - ADTKVM2mDP

Version 1.01, 1 July 2026

Document reference: AISEP-CC-CR-2026-EFT-T052-CR-V1.01
(Certification expires five years from certification report date)

Table of contents

Executive Summary

This report describes the findings of the IT security evaluation of Advanced Design Technology Pty Ltd, ADT WASP - ADTKVM2mDP against Common Criteria approved *Protection Profiles (PPs).*

The Target of Evaluation (TOE) is a KVM appliance belonging to the PSD family, designed to connect a single set of peripherals, such as 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 two 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 model designation for the TOE is ADTKVM2mDP.

This report concludes that the TOE has complied with the following *PPs [4]:*

- *Protection Profile for Peripheral Sharing Device, Version 4.0, 19 July 2019 (PP_PSD_V4.0)*
- *PP-Module for Video/Display Devices, Version 1.0, 19 July 2019 (MOD_VI_V1.0)*
- *PP-Module for Keyboard/Mouse Devices, Version 1.0, 19 July 2019 (MOD_KM_V1.0).*

Additionally, the above PPs are grouped together using a certified PP-Configuration. This evaluation used the following *PP-Configuration [4.d]:*

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

The evaluation was conducted in accordance with the Common Criteria and the requirements of the *Australian Information Security Evaluation Program (AISEP).* The evaluation was performed by Teron Labs with the final *Evaluation Technical Report (ETR) [7]* submitted on 16 May 2026.

With regard to the secure operation of the TOE, the Australian Certification Authority recommends that the users note the following:

- Potential users of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.
- The users should make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings.
- Users should be aware that only connected PCs running the Windows operating system are supported.
- Users of the TOE should regularly inspect tamper-evident seals, which have proved to be reliable to detecting physical tampering.
- The TOE includes an internal battery to maintain configuration settings, which may deplete and affect operation. If this occurs, return to ADT for remediation.
- Once an operational environment is set up with the TOE powered on and PCs connected, it is recommended to keep the environment as consistent as possible. If the environment is to be changed, power off the TOE and connected PCs until the environment is set up once again.

- If inconsistencies are encountered during operation of the TOE, a power-cycle via unplugging and re-plugging the USB-C cables (power-supply) of the TOE is found to mitigate such encounters.
- The use of USB audio headsets should be prohibited within the evaluated configuration.
- The connection of any device that bypasses the TOE or implements disallowed protocols or services is prohibited. This includes USB cameras, wireless devices, USB storage, PS/2 peripherals, and unauthorised composite devices.
- Mouse and Keyboard peripherals with multiple functionalities, such as those with internal storage, are not guaranteed to be supported.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the *Security Target [8]* and read this Certification Report prior to deciding whether to purchase the product.

Introduction

Overview

This chapter contains information about the purpose of this document and how to identify the TOE.

Purpose

The purpose of this Certification Report is to:

- report the certification of results of the IT security evaluation of the TOE against the requirements of the *Common Criteria [1,2,3]* and *Protection Profiles [4]*
- provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's *Security Target [8]* which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

Identification

The TOE is the ADT WASP - ADTKVM2mDP.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	ADT WASP - ADTKVM2mDP
TOE Type	Peripheral Sharing Device
Hardware platforms	ADTKVM2mDP
TOE Software	ADT WASP Firmware 1.0
Security Target	ADT WASP Security Target, Version 1.0.3, 30 June 2026
Evaluation Technical Report	Evaluation Technical Report 1.0, dated 16 May 2026 Document reference EFT-T052-ETR 1.0
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, April 2017, Version 3.1 Rev 5
Methodology	Common Methodology for Information Technology Security, April 2017 Version 3.1 Rev 5

Conformance	▪ Protection Profile for Peripheral Sharing Device, Version 4.0, 19 July 2019 (PP_PSD_V4.0) ▪ PP-Module for Video/Display Devices, Version 1.0, 19 July 2019 (MOD_VI_V1.0) ▪ PP-Module for Keyboard/Mouse Devices, Version 1.0, 19 July 2019 (MOD_KM_V1.0) ▪ PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, and Video/Display Devices, Version: 1.0,19 July 2019 (CFG_PSD-KM-VI_V1.0).
Developer	Advanced Design Technology (ADT) 24 Kembla St, Fyshwick ACT 2601 Australia
Evaluation facility	Teron Labs Level 2, 14 Moore St, Canberra ACT 2601 Australia

Target of Evaluation

Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, the scope of evaluation, its security policies and its secure usage.

Description of the TOE

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 two 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.

TOE Functionality

The TOE functionality that was evaluated is described in section 1.4 of the *Security Target [8].*

TOE Physical Boundary

The physical boundary of the TOE includes all hardware and software parts and the security guidance of the TOE. The parts of the TOE included in the physical boundary are detailed in *Table 1*.

Part of the TOE	Identification	Description
TOE Hardware	ADTKVM2mDP	The hardware platform and the casing of the TOE. Includes the processor, the memories, and the persistent storage.
TOE Software	ADT WASP Firmware 1.0	This firmware is embedded in the TOE hardware and is not modifiable.

Security Guidance	Guidance Document, KVM Project, ADT WASP - ADTKVM2mDP, Version 2.2, 30 June 2026	The Common Criteria Guidance supplement for the TOE. The security guidance is distributed as a document in PDF format.

Table 1 -Parts Included in the physical boundary of the TOE

TOE Hardware is the platform on which the TOE Software is executed. Only the platforms identified in *Table 1* are included in the evaluation.

Clarification of Scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The scope of the evaluation was limited to those claims made in the *Security Target [8].*

Evaluated Functionality

Functional tests performed during the evaluation were taken from the *Protection Profiles [4]* and *PP Supporting Documents [12]* and sufficiently demonstrate the security functionality of the TOE. Some of the tests were combined for ease of execution.

Non-TOE Hardware/Software/Firmware

The TOE does not require additional hardware, software or firmware to operate.

Non-evaluated Functionality and Services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

Australian Government users should refer to the *Australian Government Information Security Manual [5]* for policy relating to using an evaluated product in an unevaluated configuration.

The following components are considered outside of the scope of the TOE:

- USB Audio headsets not allowed to be used for the evaluated configuration.
- Users must not connect any device to the TOE, its connected hosts, or peripherals that bypass the TOE or implement disallowed protocols or services. This includes USB still or streaming cameras, wireless devices, USB mass storage devices, PS/2 peripherals, and any unauthorized composite or multifunction devices.

TOE Security Policy

The TOE Security Policy is a set of rules that defines the required security behaviour of the TOE; how information within the TOE is managed and protected. The *Security Target [8]* contains a summary of the functionality that is evaluated.

Secure Delivery

The TOE delivery and installation procedure is described the *Configuration Guide [6]*. The configuration guide outlines the following methods for delivery of the TOE, as agreed between ADT and the customer:

- Courier delivery
- Hand delivery
- Customer collection

Prior to installing or using the KVM, KVM should be inspected to ensure it has not been tampered with.

Users should routinely inspect the equipment seals of the unit and immediately request replacement of the KVM if the labels have been damaged or removed. Do not attempt to re-apply or remove a seal, only the manufacturer (ADT) may re-apply seals.

Installation of the TOE

The *Configuration Guide [6]* contains all relevant information for the secure configuration of the TOE.

Product Verification

Users should conduct a pre-use inspection as described in this section.

Confirm the KVM label, located under the unit and engraved into the chassis, an example of which is shown below:

The label shows the manufacturer (Advanced Design Technology, ADT) and logo, the P/N (ADTKVM2mDP) (being a 2 port KVM with mini DisplayPort connectors), a serial number of the form (xx)xxx, where x is an alphanumeric character (except the letters “O” / “o” and “I” / “i”), the ADT NATO manufacturer code (“NCAGE”) (Z19D1) and the year of manufacture (yyyy).

Documentation and Guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is provided with the TOE when the TOE is purchased by the consumer, and it titled as follows:

- *Guidance Document, KVM Project, ADT WASP - ADTKVM2mDP, version 2.2, 30 June 2026* [6].

All Common Criteria guidance material is available at *https://www.commoncriteriaportal.org [1, 2, 3, 9, and 13].*

The *Australian Government Information Security Manual* is available at *https://www.cyber.gov.au/ism [5].*

Secure Usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

The TOE is assumed to be physically secured within its operational environment, protected from physical attacks that could compromise its security or interfere with its physical connections and correct operation. This level of protection is expected to be sufficient to safeguard the device and the sensitive data it handles.

The TOE is expected to provide Peripheral Sharing Device functionality as its primary purpose and should not offer any general-purpose computing capabilities.

The operational environment where the TOE operates is assumed to exclude the use of wireless peripheral devices. All authorised peripherals connected to the PSD are expected to utilise wired interfaces only.

The TOE users are assumed to be trustworthy and to operate the device in accordance with all applicable guidance documentation. This includes adhering to organisational security policies, applying configuration guidance correctly, and maintaining appropriate operational practices.

The TOE users are assumed to be authorised to interact with all computers connected to the device. The TOE does not enforce user-level access control between connected systems, nor does it restrict or mediate user interactions with those systems.

The computers connected to the TOE are assumed not to be equipped with specialised data acquisition or signal processing peripherals. This includes, but is not limited to, analog-to-digital conversion interfaces, high-performance audio interfaces, digital signal processing components, or analog video capture capabilities.

Evaluation

Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

Evaluation Procedures

The criteria against which the TOE has been evaluated are contained in the relevant *Protection Profiles [4]* and *Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5, Parts 2 and 3 [1, 2].*

Testing methodology was drawn from *Common Methodology for Information Technology Security, April 2017 Version 3.1 Revision 5 [3]* and relevant *Supporting Documents [12].*

The evaluation was carried out in accordance with the operational procedures of the *Australian Information Security Evaluation Program [10]*.

In addition, the conditions outlined in the *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security [9]* and the document *CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs [13]* were also upheld.

Functional Testing

All functional tests performed by the evaluators were taken from the base *Protection Profile [4.a]* and *Supporting Documents [12.a, 12.b].* The tests were designed to provide the required testing coverage for the security functions claimed by the TOE.

Isolation Testing

The isolation design, including the design description, justification of isolation mechanisms, and firmware dependencies, has been assessed by the evaluators based on detailed *vendor-supplied documentation [11].*

This documentation meets the requirements of the *base Protection Profile [4.a]* for demonstrating effective data isolation between connected systems.

Penetration Testing

The evaluators performed the evaluation activities for vulnerability assessment specified by the *Peripheral Switch Device Protection Profile and Protection Profile Modules [4.a, 4.b, 4.c].* The evaluators have examined the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the *ST [8].* The evaluators examined the TOE and confirmed that it had been installed properly and was in a known state.

The evaluators performed a search of publicly available information for known or potential vulnerabilities in the TOE and supporting components. The evaluators performed a CVE search, with keywords compiled based on discussion with the vendor of hardware materials used, and known functionality. No CVE results were found based on these keywords. The latest search occurred on **27 February 2026**.

Based on the results of this testing, the evaluators determined that the TOE is resistant to an attacker possessing a basic attack potential.

Certification

Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

Assurance

This certification is focused on the evaluation of product compliance with Protection Profiles that cover the technology area of peripheral sharing devices with added security functionality including Keyboard and Mouse Device functions and Video/Display Device functions. Organisations can have confidence that the scope of an evaluation against an ASD-approved Protection Profile covers the necessary security functionality expected of the evaluated product and known threats will have been addressed.

The analysis is supported by testing as outlined in the base PP and Protection Profile Module activities, and a vulnerability survey demonstrating resistance to penetration attackers with a basic attack potential. Compliance also provides assurance through evidence of secure delivery procedures.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with the *Protection Profiles (PPs) [4].* PPs provide assurance by providing a full Security Target, and an analysis of the Security Functional Requirements in that *Security Target [8]* and *guidance documentation [6]* of the TOE.

Certification Result

Teron Labs **has determined** that the TOE upholds the claims made in the *Security Target [8]* and **has met** the requirements of the Protection Profiles *PP_PSD_V4.0 [4.a], MOD_KM_V1.0 [4.b], MOD_VI_V1.0 [4.c] and PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, and Video/Display Devices [4.d].*

After due consideration of the conduct of the evaluation as reported to the certifiers, and of the *Evaluation Technical Report [7],* the Australian Certification Authority **certifies** the evaluation of the ADT WASP - ADTKVM2mDP performed by the Australian Information Security Evaluation Facility, Teron Labs.

The Australian Certification Authority certifies that the *Security Target [8]* have met the requirements of the Peripheral Sharing Device *Protection Profiles [4].*

Certification is not a guarantee of freedom from security vulnerabilities.

Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian Government users. For further guidance, Australian Government users should refer to the *Australian Government Information Security Manual [5].*

In addition to ensuring that the assumptions concerning the operational environment are fulfilled, and the guidance document is followed, the Australian Certification Authority also recommends the users to note the following:

- Potential users of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

- The users should make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings.
- Users should be aware that only connected PCs running the Windows operating system are supported.
- Users of the TOE should regularly inspect tamper-evident seals, which have proved to be reliable to detecting physical tampering.
- The TOE includes an internal battery to maintain configuration settings, which may deplete and affect operation. If this occurs, return to ADT for remediation.
- Once an operational environment is set up with the TOE powered on and PCs connected, it is recommended to keep the environment as consistent as possible. If the environment is to be changed, power off the TOE and connected PCs until the environment is set up once again.
- If inconsistencies are encountered during operation of the TOE, a power-cycle via unplugging and re-plugging the USB-C cables (power-supply) of the TOE is found to mitigate such encounters.
- The use of USB audio headsets should be prohibited within the evaluated configuration.
- The connection of any device that bypasses the TOE or implements disallowed protocols or services is prohibited. This includes USB cameras, wireless devices, USB storage, PS/2 peripherals, and unauthorised composite devices.
- Mouse and Keyboard peripherals with multiple functionalities, such as those with internal storage, are not guaranteed to be supported.

Annex – References and Abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April 2017, Version 3.1 Revision 5*
2. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5*
3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5*
4. Protection Profiles:
    a) *Protection Profile for Peripheral Sharing Device, Version 4.0, 19 July 2019 (PP_PSD_V4.0)*
    b) *PP-Module for Video/Display Devices, Version 1.0, 19 July 2019 (MOD_VI_V1.0)*
    c) *PP-Module for Keyboard/Mouse Devices, Version 1.0, 19 July 2019 (MOD_KM_V1.0)*
    d) *PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, and Video/Display Devices, Version: 1.0,19 July 2019 (CFG_PSD-KM-VI_V1.0).*
5. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism
6. *Guidance Document, KVM Project, ADT WASP - ADTKVM2mDP, Version 2.2, 30 June 2026*
7. *Evaluation Technical Report, ADT WASP - ADTKVM2mDP, Version 1.0, 16 May 2026* (Document reference EFT-T052-ETR 1.0)
8. *Security Target for ADT WASP - ADTKVM2mDP, Version 1.0.3, 30 June 2026*
9. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 July 2014*
10. *AISEP Policy Manual (APM): https://www.cyber.gov.au/sites/default/files/2023-03/2022_AUG_REL_AISEP_Policy_Manual_6.3.pdf*
11. Isolation Documentation:
    a) *Isolation Document, KVM Project, ADT WASP - ADTKVM2mDP, version 2.0, 08 May 2026*
12. Protection Profile Supporting Documents
    a) *Supporting Document, Supporting Document, Mandatory Technical Document, PP-Module for Video/Display Devices, Version 1.0, 19-July-2019 (MOD_VI_V1.0_SD)*
    b) *Supporting Document, Mandatory Technical Document, PP-Module for Keyboard/Mouse Devices, Version 1.0, 19-July-2019 (MOD_KM_V1.0_SD).*
13. *CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs 30 September 2021, Version 2.0, CCDB-013-v2.0*

Abbreviations

AISEP	Australian Information Security Evaluation Program
ADT	Advanced Design Technology (TOE Vendor)
ASD	Australian Signals Directorate
ASIC	Application Specific Integrated Circuit
CCRA	Common Criteria Recognition Arrangement
HID	Human Interface Device
IT	Information Technology
KVM Switch	Keyboard, Video and Mouse Switch
MST	Multi-Stream Transport
PCs	Personal Computer(s)
P/N	Part Number
PP	Protection Profile
PSD	Peripheral Sharing Device
PS/2	PS/2 is a 6-pin mini-DIN connector used for connecting keyboards/mouse to a PC
TOE	Target of Evaluation
USB	Universal Serial Bus

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate