



Communications
Security Establishment

Centre de la sécurité
des télécommunications

CANADIAN CENTRE^{FOR} **CYBER SECURITY**

COMMON CRITERIA CERTIFICATION REPORT

Protection Profile for Peripheral Sharing Device version 4.0, 19 July 2019

27 May 2021

CCCS-PP-006-CR

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The Protection Profile identified in this certification report has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security (CCCS). This certification report applies only to the identified version and release of the Protection Profile. The evaluation has been conducted in accordance with the provisions of the Canadian CC Scheme, and the conclusions of the testing laboratory in the evaluation report are consistent with the evidence adduced.

If your organization has identified a requirement for this certification report and would like more detailed information, please contact:

Canadian Centre for Cyber Security

Contact Centre and Information Services

contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

OVERVIEW

The Canadian Common Criteria Scheme provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Testing Laboratory (CCTL) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCTL is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

This certification report is posted to the Common Criteria portal (the official website of the International Common Criteria Program).

TABLE OF CONTENTS

Executive Summary	5
1 Identification	6
2 PP Description	7
3 Security Problem Description and Objectives	8
3.1 Assumptions	8
3.2 Threats	8
3.3 Organizational Security Policies	9
3.4 Security Objectives	9
4 Security Requirements	12
4.1 Security Functional Requirements	12
4.2 Security Assurance Requirements	14
5 Results of the Evaluation	15
6 References	16

EXECUTIVE SUMMARY

This report documents the results of the evaluation of the Protection Profile for Peripheral Sharing Device, version 4.0 (PP_PSD_v4.0). It presents a summary of the PP_PSD_v4.0 and the evaluation results. It presents a summary of the PP_PSD_v4.0 together with the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the PP_PSD_v4.0 was performed concurrent with the first product evaluation against the PP's requirements. In this case the Target of Evaluation (TOE) for this first product was the Belkin F1DN104KVM-UN-4, F1DN204KVM-UN-4, F1DN102KVM-UN-4, F1DN202KVM-UN-4, F1DN108KVM-UN-4, F1DN208KVM-UN-4, F1DN116KVM-UN-4 Firmware Version 44444-E7E7 Peripheral Sharing Devices (hereafter referred to as "Belkin KVM Devices"). The evaluation was performed by the EWA-Canada Common Criteria Testing Laboratory and was completed in April 2021. This evaluation addressed the base requirements of PP_PSD_v4.0, as well as the requirements contained in Appendices A and B.

An additional evaluation of the PP was performed by the EWA-Canada Common Criteria Testing Laboratory to confirm that it meets the claimed APE assurance requirements.

The evaluations determined that the PP_PSD_v4.0 is both Common Criteria Part 2 Extended and Part 3 Conformant. The Security Target contains material drawn directly from the PP_PSD_v4.0 as well as the following: PP-Module for Analog Audio Output Devices version 1.0; PP-Module for Keyboard/Mouse Devices version 1.0; PP-Module for User Authentication Devices version 1.0; and PP-Module for Video/Display Devices version 1.0. Evaluation of the ST materials that relate to PP_PSD_v4.0 as part of completing the ASE work units serves to satisfy the APE work units as well.

The Canadian Centre for Cyber Security, as the Certification Body, found that the evaluations demonstrated that the PP_PSD_v4.0 meets the requirements of the APE components. The conclusions of the testing laboratory in the Assurance Activity Report (AAR) are consistent with the evidence produced.

1 IDENTIFICATION

The evaluation of the Protection Profile for Peripheral Sharing Device, version 4.0 (PP_PSD_v4.0) was performed concurrently with the first product evaluation against the PP. The Target of Evaluation (TOE) was the Belkin F1DN104KVM-UN-4, F1DN204KVM-UN-4, F1DN102KVM-UN-4, F1DN202KVM-UN-4, F1DN108KVM-UN-4, F1DN208KVM-UN-4, F1DN116KVM-UN-4 Firmware Version 44444-E7E7 Peripheral Sharing Devices (hereafter referred to as “Belkin KVM Devices”) which was evaluated for conformance to the PP-Configuration for Peripheral Sharing Device, Analog Audio Output Devices, Keyboard/Mouse Devices, User Authentication Devices, and Video/Display Devices, version 1.0 (PP-Config. for PSD-AO-KM-UA-VI_v1.0). The evaluation was performed by the EWA-Canada Common Criteria Testing Laboratory and was completed in April 2021.

The PP_PSD_v4.0 contains a set of “base” requirements that all conformant STs must include, and additionally contains “Optional” and “Selection-based” requirements. The PP contains Implementation-Dependent Optional Requirements that are dependent on the TOE implementing a particular function. The Selection-based requirements are additional requirements based on selections made within the body of the PP; if certain selections are made, then additional requirements will need to be included.

The following identifies the PP that was the subject of the evaluation and certification, together with supporting information from the base evaluation performed against this PP.

Protection Profile	Protection Profile for Peripheral Sharing Device version 4.0
Security Target	Belkin F1DN104KVM-UN-4, F1DN204KVM-UN-4, F1DN102KVM-UN-4, F1DN202KVM-UN-4, F1DN108KVM-UN-4, F1DN208KVM-UN-4, F1DN116KVM-UN-4 Firmware Version 44444-E7E7 Peripheral Sharing Devices Security Target, Version 1.4B, 19 February 2021
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
CC Testing Lab	EWA-Canada

2 PP DESCRIPTION

The PP_PSD_v4.0 describes common security requirements for Peripheral Sharing Devices (PSDs). In the context of this PP, a PSD is an IT product for securely connecting one or more peripheral devices to one or more computers such that data cannot flow between computers by way of the peripherals or the PSD. Examples of PSDs that can claim compliance to this PP include Keyboard, Video, Mouse (KVM) switches; Keyboard, Mouse (KM) switches; and Isolators.

A PSD may be composed of one or more hardware components or platforms, and its software or firmware. It may include cables and accessories. PSDs that support more than one computer include a user interface that includes a visible indication of the selected computer interface and a mechanism for changing the selected computer interface. The user interface can be implemented on the chassis of the PSD using, for example, a touch screen or lights and buttons, or as part of a wired remote control.

3 SECURITY PROBLEM DESCRIPTION AND OBJECTIVES

3.1 ASSUMPTIONS

The specific conditions listed here are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: Assumptions

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

3.2 THREATS

TOEs conforming to the PP_PSD_v4.0 counter the following threats.

Table 2: Threats

Threat Name	Threat Definition
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.

Threat Name	Threat Definition
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.

3.3 ORGANIZATIONAL SECURITY POLICIES

No organizational security policies have been identified that are specific to Peripheral Sharing Devices.

3.4 SECURITY OBJECTIVES

The following table contains security objectives for the TOE.

Table 3: TOE Security Objectives

TOE Security Objective	TOE Security Objective Definition
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 TOE is powered. (Addressed by: FDP_APC_EXT.1)
O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED	The PSD shall not allow data to transit 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)

TOE Security Objective	TOE Security Objective Definition
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 buttons, console switches, console touch screen, wired remote control, and peripheral devices using a guard. Unauthorized switching mechanisms include keyboard shortcuts, also known as "hotkeys," automatic port scanning, control through a connected computer, and control through keyboard shortcuts. Where applicable, the results of the switching activity shall be indicated by the TSF so that it is clear to the user that the switching mechanism was engaged as intended. A conformant TOE may also provide a management function to configure some aspects of the TSF. If the TOE provides this functionality, it shall ensure that whatever management functions it provides can only be performed by authorized administrators and that an audit trail of management activities is generated. (Addressed by: 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 labeled with at least one visible unique identifying tamper-evident marking that can be used to authenticate the device. The PSD manufacturer must maintain a complete list of manufactured PSD articles and their respective identification markings' unique identifiers. (Addressed by: 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))

TOE Security Objective	TOE Security Objective Definition
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)

The following table contains security objectives for the Operational Environment.

Table 4: Environmental Security Objectives

Environmental Security Obj.	Environmental Security Objective Definition
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.

4 SECURITY REQUIREMENTS

4.1 SECURITY FUNCTIONAL REQUIREMENTS

As indicated above, requirements in the PP_PSD_v4.0 are comprised of the “base” requirements and additional requirements that are conditionally optional. The following table contains the “base” requirements that were certified as part of the Belkin KVM Devices evaluation activity referenced above.

Table 5: “Base” Security Functional Requirements

Requirement Class	Requirement Component	Verified By
FDP: User Data Protection	FDP_APC_EXT.1: Active PSD Connections	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
	FDP_PDC_EXT.1: Peripheral Device Connection	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
	FDP_RIP_EXT.1: Residual Information Protection	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
	FDP_SWI_EXT.1: PSD Switching	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
FPT: Protection of the TSF	FPT_FLS_EXT.1: Failure with Preservation of Secure State	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
	FPT_NTA_EXT.1: No Access to TOE	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
	FPT_PHP.1: Passive Detection of Physical Attack	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
	FPT_TST.1: TSF Testing	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
	FPT_TST_EXT.1: TSF Testing	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)

The following table contains the “Optional” requirements contained in Appendix A, and an indication of which evaluation those requirements were verified in. These requirements were certified as part of the Belkin KVM Devices evaluation activity referenced above.

Table 6: “Optional” Security Functional Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
FDP: User Data Protection	FDP_RIP_EXT.2: Purge of Residual Information	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
FIA: Identification and Authentication	FIA_UAU.2: User Authentication Before Any Action	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
	FIA_UID.2: User Identification Before Any Action	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
FMT: Security Management	FMT_MOF.1: Management of Security Functions Behaviour	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
	FMT_SMF.1: Specification of Management Functions	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
	FMT_SMR.1: Security Roles	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
FPT: Protection of the TSF	FPT_PHP.3: Resistance to Physical Attack	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
	FPT_STM.1: Reliable Time Stamps	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)

The following table contains the “Selection-Based” requirements contained in Appendix B, and an indication of which evaluation those requirements were verified in. These requirements were certified as part of the Belkin KVM Devices evaluation activity referenced above.

Table 7: “Selection-Based” Security Functional Requirements

Requirement Class	Requirement Component	Verified By
FDP: User Data Protection	FDP_SWI_EXT.2: PSD Switching Methods	ST: Belkin KVM Devices (PP-Config. For PSD-AO-KM-UA-VI_v1.0)
FTA: TOE Access	FTA_CIN_EXT.1 : Continuous Indications	ST: Belkin KVM Devices (PP-Config. For PSD-AO-KM-UA-VI_v1.0)

4.2 SECURITY ASSURANCE REQUIREMENTS

The following are the assurance requirements contained in the PP_PSD_v4.0:

Table 8: Security Assurance Requirements

Requirement Class	Requirement Component	Verified By
ASE: Security Target	ASE_CCL.1: Conformance Claims	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
	ASE_ECD.1: Extended Components Definition	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
	ASE_INT.1: ST Introduction	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
	ASE_OBJ.2: Security Objectives	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
	ASE_REQ.2: Derived Security Requirements	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
	ASE_SPD.1: Security Problem Definition	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
	ASE_TSS.1: TOE Summary Specification	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
ADV: Development	ADV_FSP.1: Basic Functional Specification	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
AGD: Guidance Documents	AGD_OPE.1: Operational User Guidance	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
	AGD_PRE.1: Preparative Procedures	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
ALC: Life Cycle Support	ALC_CMC.1: Labeling of the TOE	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
	ALC_CMS.1: TOE CM Coverage	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
ATE: Tests	ATE_IND.1: Independent Testing – Conformance	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0)

5 RESULTS OF THE EVALUATION

Note that for APE elements and work units that are identical to ASE elements and work units, the testing laboratory performed the APE work units concurrent to the ASE work units. In addition, the testing laboratory performed a separate APE evaluation of the PP_PSD_v4.0 that was independent of the product evaluation.

Table 9: Evaluation Results

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1: Conformance Claims	Pass	- ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0) - APE Evaluation
APE_ECD.1: Extended Components Definition	Pass	- ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0) - APE Evaluation
APE_INT.1: PP Introduction	Pass	- ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0) - APE Evaluation
APE_OBJ.2: Security Objectives	Pass	- ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0) - APE Evaluation
APE_REQ.2: Derived Security Requirements	Pass	- ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0) - APE Evaluation
APE_SPD.1: Security Problem Definition	Pass	- ST: Belkin KVM Devices (PP-Config. for PSD-AO-KM-UA-VI_v1.0) - APE Evaluation

6 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Protection Profile for Peripheral Sharing Device, Version 4.0, 19 July 2019.
Belkin F1DN104KVM-UN-4, F1DN204KVM-UN-4, F1DN102KVM-UN-4, F1DN202KVM-UN-4, F1DN108KVM-UN-4, F1DN208KVM-UN-4, F1DN116KVM-UN-4 Firmware Version 44444-E7E7 Peripheral Sharing Devices Security Target, Version 1.4B, 19 February 2021.
Assurance Activity Report Belkin F1DN104KVM-UN-4, F1DN204KVM-UN-4, F1DN102KVM-UN-4, F1DN202KVM-UN-4, F1DN108KVM-UN-4, F1DN208KVM-UN-4, F1DN116KVM-UN-4 Firmware Version 44444-E7E7 Peripheral Sharing Devices, Version 1.1, 29 April 2021.