National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Protection Profile for Peripheral Sharing Switch, Version 1.3, February 13, 2015

Report Number: CCEVS-VR-PP-0021
Dated: April 13, 2016
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

Base and Additional Requirements
Computer Sciences Corporation.
Hanover, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Protection Profile for Peripheral Sharing Switch, Version 3.0 (PPPSS3.0). It presents a summary of the PPPSS30 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the PPPSS30 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 High Security Labs Secure KM. The evaluation was performed by CSC Global Cybersecurity, Security Testing & Certification Lab in Hanover, Maryland, in the United States and was completed in March 2016. This evaluation addressed the base requirements of the PPPSS30, as well as a few of the optional and selection-based requirements from Annex F and G.

The information in this report is largely derived from the Assurance Activity Report (AAR), written by the Computer Sciences Corporation.

The evaluation determined that the PPPSS30 is both Common Criteria Part 2 Extended and Part 3 Conformant. The PP identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). Because the ST contains only material drawn directly from the PPPSS30, performance of the majority of the ASE work units serves to satisfy the APE work units as well. Where this is not the case, the lab performed the outlying APE work units as part of this evaluation.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team found that the evaluation showed that the PPPSS30 meets the requirements of the APE components. These findings were confirmed by the VR author. The conclusions of the testing laboratory in the assurance activity report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profiles containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of the PPPSS30 was performed concurrent with the first product evaluation against the PP. In this case the TOE for this first product was the High Security Labs Secure KM Switch, provided by High Security Labs. The evaluation was performed by CSC Global Cybersecurity, Security Testing & Certification Lab in Hanover, Maryland, in the United States and was completed in March 2016.

The PPPSS30 contains a set of "base" requirements that all conformant STs must include as well as "additional" requirements that are either optional or selection-based, depending on the requirement in question. The vendor may choose to include such requirements in the ST and still claim conformance to this PP. If the vendor's TOE performs capabilities that are governed by any additional requirements, that vendor is expected to claim all of the additional requirements that relate to these capabilities.

Because these additional requirements may not be included in a particular ST, the initial use of the PP will address (in terms of the PP evaluation) the base requirements as well as any additional requirements that are incorporated into that initial ST. Subsequently, TOEs that are evaluated against the PPPSS30 that incorporate additional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and any appropriate updates to this validation report will be made.

The following identifies the PP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this PP, as well as subsequent evaluations that address additional requirements in the PPPSS30.

Protection Profile	*Protection Profile for Peripheral Sharing Switch, Version 3.0, February 12, 2015*
ST (Base)	High Security Labs Secure KM Security Target, Version 3.14, January 28, 2016
ST (Additional)	N/A
Assurance Activity Report (Base)	HSL Secure KM Switch Assurance Activity Report version 1.0, February, 2016
Assurance Activity Report (Additional)	N/A
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
CCTL (base and additional)	Computer Sciences Corporation, Hanover, MD USA
CCEVS Validators (base)	Chris Thorpe Daniel Faigin Ken Stutterheim Tony Chew Brad O'Neill
CCEVS Validators (Additional)	N/A

3 PPPSS Description

This Protection Profile (PP), describing security requirements for a Peripheral Sharing Switch (PSS), defined to provide a mechanism to securely connect a common set of peripherals to the attached computer(s), is intended to provide a minimal, baseline set of requirements that are targeted at mitigating well-defined and described threats. It represents an evolution of

"traditional" Protection Profiles and the associated evaluation of the requirements contained within the document.

In the context of this PP, a peripheral sharing switch provides a mechanism to securely connect a common set of peripherals (1 to n) to the attached computer(s) (1 to j) without sharing or transferring data. The PSS will follow a deliberate action from the user to enable an interaction between the connected peripherals and the selected computer. Examples of the type of PSS that should claim compliance to this PP include keyboard, video, mouse (KVM) switches; keyboard, mouse (KM) switches; isolators (PSS with a single connected computer); and combiners (PSS capable of displaying multiple computers in one video display). Examples of devices that are not suitable for evaluation against this PP include Internet Protocol (IP) and network-attached switches and matrix switches

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's 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.

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

Table 1: Assumptions

4.2 Threats

Threat Name	Threat Definition
T.DATA_LEAK	A connection via the PSS between computers may allow unauthorized data flow through the PSS or its connected peripherals.
T.SIGNAL_LEAK	A connection via the PSS between computers may allow unauthorized data flow through bit-by-bit signaling.
T.RESIDUAL_LEAK	A PSS may leak (partial, residual, or echo) user data between the intended connected computer and another

Threat Name	Threat Definition
	unintended connected computer. More specifically, a PSS may leak user keyboard entries to a PSS-connected computer other than the selected computer in real-time or at a later time.
T.UNINTENDED_SWITCHING	A threat in which the user is connected to a computer other than the one to which they intended to be connected.
T.UNAUTHORIZED_DEVICES	The use of an unauthorized peripheral device with a specific PSS peripheral port may allow unauthorized data flows between connected devices or enable an attack on the PSS or its connected computers.
T.AUTHORIZED_BUT_UNTRUSTED_DEVICES	The use of an authorized peripheral device with the PSS may still cause unauthorized data flows between connected devices or enable an attack on the PSS or its connected computers. Such threats are possible due to known or unknown device vulnerabilities or due to additional functions within the authorized peripheral device.
T.LOGICAL_TAMPER	An attached device (computer or peripheral) with malware, or otherwise under the control of a malicious user, could modify or overwrite code embedded in the TOE's volatile or non-volatile memory to allow unauthorized information flows between connected devices.
T.PHYSICAL_TAMPER	A malicious human agent could physically tamper with or modify the TOE to allow unauthorized information flows between connected devices.
T.REPLACEMENT	A malicious human agent could replace the TOE during shipping, storage, or use with an alternate device that does not enforce the TOE security policies.
T.FAILED	Detectable failure of a PSS may cause an unauthorized information flow, weakening of PSS security functions, or unintended switching.

Table 2: Threats

4.3 Organizational Security Policies

The PPPSS30 does not define organizational security policies.

4.4 Security Objectives

The following table contains security objectives for the TOE.

TOE Security Obj.	TOE Security Objective Definition
O.COMPUTER_INTERFACE_ISOLATION	The TOE must prevent unauthorized data flow to assure that the TOE and/or its connected peripheral devices would not be exploited in an attempt to leak data. The TOE computer interface shall be isolated from all other TOE computer interfaces while TOE is powered.

TOE Security Obj.	TOE Security Objective Definition
O.COMPUTER_INTERFACE_ISOLATION_TOE_ UNPOWERED	The same level of isolation defined in the dataflow objectives must be maintained at all times, including periods while TOE is unpowered.
O.USER_DATA_ISOLATION	User data such as keyboard entries should be switched (i.e., routed) by the TOE only to the computer selected by the user. The TOE must provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.
O.NO_USER_DATA_RETENTION	The TOE shall not retain user data after it is powered down.
O.PURGE_TOE_KB_DATA_WHILE_SWITCHING	The TOE shall purge all user keyboard data from computer interfaces following channel switching and before interacting with the new connected computer.
O.NO_DOCKING_PROTOCOLS	The use of docking protocols such as DockPort, USB docking, Thunderbolt etc. is not allowed in the TOE.
O.NO_OTHER_EXTERNAL_INTERFACES	The TOE may not have any wired or wireless external interface with external entities (external entity is an entity outside the TOE evaluated system, its connected computers and peripheral devices).
O.NO_ANALOG_AUDIO_INPUT	Shared audio input peripheral functions (i.e., analog audio microphone input or line input) are not allowed in the TOE
O.UNIDIRECTIONAL_AUDIO_OUT	The TOE shall be designed to assure that reverse audio signal attenuation will be at least 30 dBv measured with 200 mV and 2V input pure sine wave at the extended audio frequency range including negative swing signal. The level of the reverse audio signal received by the selected computer shall be minimal to assure that the signal level generated by headphones will be well under the noise floor level.
O.COMPUTER_TO_AUDIO_ISOLATION	The audio dataflow shall be isolated from all other TOE functions. Signal attenuation between any TOE computer interface and any TOE audio interface shall be at least 45 dBv measured with 2V input pure sine wave at the extended audio frequency range including negative swing signal.
O.USER_AUTHENTICATION_ISOLATION	The user authentication function shall be isolated from all other TOE functions.
O.USER_AUTHENTICATION_RESET	Unless the TOE emulating the user authentication function, upon switching computers, the TOE shall reset (turn off and then turn on) the power supplied to the user authentication device for at least 1 second.
O.USER_AUTHENTICATION_TERMINATION	If the TOE is emulating the user authentication (instances of the user authentication device are coupled to multiple computers at the same time) then once the authentication session is terminated.
O.USER_AUTHENTICATION_ADMIN	If the TOE is capable of being configured after deployment with user authentication device

TOE Security Obj.	TOE Security Objective Definition
	qualification parameters then such configuration may only performed by an administrator.
O.AUTHORIZED_SWITCHING	The TOE shall allow only authorized switching mechanisms to switch between connected computers and shall explicitly prohibit or ignore unauthorized switching mechanisms.
O.NO_AMBIGUOUS_CONTROL	If the TOE allows more than one authorized switching mechanism, only one method shall be operative at any given time to prevent ambiguous commands.
O.CONTINUOUS_INDICATION	The TOE shall provide continuous visual indication of the computer to which the user is currently connected.
O.KEYBOARD_AND_MOUSE_TIED	The TOE shall ensure that the keyboard and mouse devices are always switched together
O.NO_CONNECTED_COMPUTER_CONTROL	The TOE shall not allow TOE control through a connected computer.
O.PERIPHERAL_PORTS_ISOLATION	The TOE shall prevent data flow between peripheral devices of different SPFs and the TOE peripheral device ports of different SPFs shall be isolated.
O.DISABLE_UNAUTHORIZED_PERIPHERAL	The TOE shall only allow authorized peripheral device types (See Annex C) per peripheral device port; all other devices shall be identified and then rejected or ignored by the TOE.
O.DISABLE_UNAUTHORIZED_ENDPOINTS	The TOE shall reject unauthorized peripheral devices connected via a USB hub. Alternatively, the TOE may reject all USB hubs.
O.KEYBOARD_MOUSE_EMULATED	The TOE keyboard and pointing device functions shall be emulated (i.e., no electrical connection other than the common ground is allowed between peripheral devices and connected computers).
O.KEYBOARD_MOUSE_UNIDIRECTIONAL	The TOE keyboard and pointing device data shall be forced to unidirectional flow from the peripheral device to the switched computer only.
O.UNIDIRECTIONAL_VIDEO	TOEs that support VGA, DVI or HDMI video shall force native video peripheral data (i.e., red, green, blue, and TMDS lines) to unidirectional flow from the switched computer to the connected display device.
O.UNIDIRERCTIONAL_EDID	TOEs that support VGA, DVI, DisplayPort or HDMI video shall force the display EDID peripheral data channel to unidirectional flow and only copy once from the display to each one of the appropriate computer interfaces during the TOE power up or reboot sequence. The TOE must prevent any EDID channel write transactions initiated by connected computers.
O.DISPLAYPORT_AUX_FILTERING	TOEs that support DisplayPort video shall prevent (i.e., filter or otherwise disable) the following auxiliary channel traffic: EDID write, USB, Ethernet, Audio return channel, UART and MCCS.

TOE Security Obj.	TOE Security Objective Definition
	Alternatively, the TOE may prevent the AUX channel from operating at Fast AUX speed (675/720 Mbps).
O.TAMPER_EVIDENT_LABEL	The TOE shall be identifiable as authentic by the user and the user must be made aware of any procedures or other such information to accomplish authentication. This feature must be available upon receipt of the TOE and continue to be available during the TOE deployment. The TOE shall be labeled with at least one visible unique identifying tamper-evident marking that can be used to authenticate the device. The TOE manufacturer must maintain a complete list of manufactured TOE articles and their respective identification markings' unique identifiers.
O.ANTI_TAMPERING	The TOE shall be physically enclosed so that any attempts to open or otherwise access the internals or modify the connections of the TOE would be evident. This shall be accomplished through the use of an always-on active antitampering system that serves to permanently disable the TOE should its enclosure be opened. The TOE shall use an always-on active antitampering system to permanently disable the TOE in case physical tampering is detected.
O.ANTI_TAMPERING_BACKUP_POWER	The anti-tampering system must have a backup power source to enable tamper detection while the TOE is unpowered.
O.ANTI_TAMPERING_BACKUP_FAIL_TRIGGER	A failure or depletion of the anti-tampering system backup power source shall trigger TOE to enter tampered state.
O.ANTI_TAMPERING_INDICATION	The TOE shall have clear user indications when tampering is detected.
O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE	Once the TOE anti-tampering is triggered, the TOE shall become permanently disabled. No peripheral-to-computer data flows shall be allowed.
O.NO_TOE_ACCESS	The TOE shall be designed so that access to the TOE firmware, software, or its memory via its accessible ports is prevented.
O.SELF_TEST	The TOE shall perform self-tests following power up or powered reset.
O.SELF_TEST_FAIL_TOE_DISABLE	Upon critical failure detection the TOE shall disable normal operation of the whole TOE or the respective failed component.
O.SELF_TEST_FAIL_INDICATION	The TOE shall provide clear and visible user indications in the case of a self-test failure.

Table 3: Security Objectives for the TOE

The following table contains objectives for the Operational Environment.

TOE Security Obj.	TOE Security Objective Definition

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

Table 4: Security Objectives for the Operational Environment

5 Requirements

As indicated above, requirements in the PPPSS30 are comprised of the "base" requirements and additional requirements that are selection based. The following are table contains the "base" requirements that were validated as part of the High Security Labs evaluation activity referenced above.

Requirement Class	Requirement Component
Base Security Functional Requirements Peripheral Sharing Switch (TOE)	
FDP: User Data Protection	FDP_IFC.1(1): Subset information flow control
	FDP_IFF.1(1): Simple security attributes
	FDP_IFC.1(2): Subset information flow control
	FDP_IFF.1(2): Simple security attributes
	FDP_ACC.1: Subset access control
	FDP_ACF.1: Security attribute based access control
	FDP_RIP.1: Subset Residual information protection
FPT: Protection of the TSF	FPT_PHP.1: Passive detection of a physical attack
	FPT_PHP.3: Resistance to physical attack
	FPT_FLS.1: Failure with preservation of secure state
	FPT_TST.1: TSF testing
FTA: TOE Access	FTA_CIN_EXT.1: Extended: Continuous Indications

Table 5: Base Requirements

The following table contains the additional selection-based requirements contained in Appendix F and G, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Requirement Class	Requirement Component	Verified By

Optional Requirements		
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	High Security Labs Secure KM Security Target, Version 3.14, January 28, 2016
FIA: Identification and Authentication	FIA_UAU.2: User identification before any action	High Security Labs Secure KM Security Target, Version 3.14, January 28, 2016
	FIA_UID.2: User identification before any action	High Security Labs Secure KM Security Target, Version 3.14, January 28, 2016
FMT: Security Management	FMT_MOF.1: Management of security functions behavior	High Security Labs Secure KM Security Target, Version 3.14, January 28, 2016
	FMT_SMF.1: Specification of Management Functions	High Security Labs Secure KM Security Target, Version 3.14, January 28, 2016
	FMT_SMR.1: Security roles	High Security Labs Secure KM Security Target, Version 3.14, January 28, 2016
Selection-Based Requirements		
FTA_ATH_EXT: User Authentication Device Reset and Termination	FTA_ATH_EXT.1: User authentication device reset	High Security Labs Secure KM Security Target, Version 3.14, January 28, 2016
	FTA_ATH_EXT.2: User authentication device session termination	

Table 6: Additional Requirements

6 Assurance Requirements

The following are the assurance requirements contained in the PPPSS30:

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1 Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance
	AGD_PRE.1: Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1: Labeling of the TOE
	ALC_CMS.1: TOE CM Coverage
ATE: Tests	ATE_IND.1: Independent Testing - Sample

Table 7: Assurance Requirements

7 Results of the evaluation

The CCTL produced an ETR that contained the following results. Note that for APE elements and work units that are identical to APE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

APE Requirement	Evaluation Verdict
APE_CCL.1	Pass
APE_ECD.1	Pass
APE_INT.1	Pass

APE_OBJ.2	Pass
APE_REQ.1	Pass
APE_SPD.1	Pass
APE_TSS.1	Pass

Table 8: Evaluation Results

8 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology as interpreted by the supplemental guidance in the PPPSS30 Assurance Activities to determine whether or not the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

9 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007.

[4] Common Criteria Project Sponsoring Organizations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] *High Security Labs Secure KM Security Target*, Version 3.14, January 28, 2016

[7] Computer Sciences Corporation, *High Security Labs Secure KM Validation Report*, Version 1.0, March 24, 2016

[8] Computer Sciences Corporation, *HSL Secure KM Switch Assurance Activity Report* Version 1.0, February 2016

[9] *Protection Profile for Peripheral Sharing Switch, Version 3.0, February 12, 2015*