Certification Report

EAL 4+ Evaluation of

Avocent®-Cybex® Secure DVI KVM Switch, Secure KM Switch and Secure Windowing KVM

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-323 CR
Version: 1.0
Date: 16 July 2012
Pagination: i to iii, 1 to 09

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment Canada.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is EWA-Canada located in Ottawa, Canada.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 16 July 2012, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

TABLE OF CONTENTS

Executive Summary

Avocent®-Cybex® Secure DVI KVM Switch, Secure KM Switch and Secure Windowing KVM (hereafter referred to as Avocent KVM Switch), from Avocent Corporation (Emerson), is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.
Avocent KVM Switch is a peripheral sharing switch. The Avocent KVM Switch allows the secure sharing of a single set of peripheral components such as Keyboard, Video Display and Mouse/Pointing devices among multiple computers through standard USB and DVI interfaces.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 03 July 2012 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Avocent KVM Switch, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 4 *augmented* assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. The following augmentation is claimed: ALC_FLR.3 – Systematic flaw remediation.

Avocent KVM Switch claims demonstrable compliance with the Peripheral Sharing Switch (PSS) Protection Profile for Human Interface Devices, version 2.1, 7 September 2010.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Avocent KVM Switch evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products List (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is Avocent®-Cybex® Secure DVI KVM Switch, Secure KM Switch and Secure Windowing KVM (hereafter referred to as Avocent KVM Switch), from Avocent Corporation (Emerson).

2 TOE Description

Avocent KVM Switch is a peripheral sharing switch. The Avocent KVM Switch allows the secure sharing of a single set of peripheral components such as Keyboard, Video Display and Mouse/Pointing devices among multiple computers through standard USB and DVI interfaces. The Avocent KVM Switch is equipped with multiple unidirectional flow forcing devices (optical data diodes) to assure adherence to the unidirectional forced data flow policy between coupled computers. The Avocent KVM Switch is available in 2, 4, 8 or 16 port models with single or dual-head (displays). Products include traditional KVM switching devices, direct display connection products (KM), remote desktop controllers (RDC) and KVM Combiners. The Remote Desktop Controller (RDC) Model RDC440 was evaluated on all models.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Avocent KVM Switch is identified in Section 6 of the ST.

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title:	Avocent®-Cybex® Secure DVI KVM Switch, Secure KM Switch and Secure Windowing KVM
Version:	1.14
Date:	03 July 2012

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.*

Avocent KVM Switch is:

a. *Common Criteria Part 2 extended;* with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
    - EXT_VIR.1 - Visual Indication Rule;
    - EXT_IUC.1 - Invalid USB Connection; and
    - EXT_ROM.1 - Read-Only Memory.
b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and
c. *Common Criteria EAL 4 augmented*, containing all security assurance requirements in the EAL 4 package, as well as the following: e.g. ALC_FLR.3 – Systematic Flaw Remediation.
d. Avocent KVM Switch claims demonstrable compliance with the Peripheral Sharing Switch (PSS) Protection profile for Human Interface Devices, version 2.1, 7 September 2010.

6 Security Policy

Avocent KVM Switch implements a Data Separation security policy to allow peripheral data to be transferred only between peripheral port groups with the same ID, as well as a unidirectional forced data flow policy to restrict data flow from shared peripherals to switched computers only; details of these security policies can be found in Section 6 of the ST.

In addition, Avocent KVM Switch implements policies pertaining to security management and protection of the TSF. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Avocent KVM Switch should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage Assumption is listed in the ST:

- The Authorized user is non-hostile and follows all usage guidance and possesses the necessary privileges to access the information transferred by the TOE.

7.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- The TOE is physically secure and is installed and managed in accordance with the manufacturer's directions.

7.3 Clarification of Scope

The TOE is intended for use by non-hostile and trained users that have followed the installation and configuration guidance provided in the product's user manual.

8 Evaluated Configuration

The evaluated configuration for Avocent KVM Switch comprises one of the following switches:

- Avocent - Cybex Secure 2-port DVI-I KVM Switch w/audio - Model SC 820D, Part number 520-933-501, Ver. 33303-C3C3;
- Avocent - Cybex Secure 4-port DVI-I KVM Switch w/audio - Model SC 840D, Part number 520-935-501, Ver. 33303-C3C3;
- Avocent - Cybex Secure 4-port DVI-I KVM Switch w/audio and DPP - Model SC 840DD, Part number 520-956-501, Ver. 33333-C3C3;
- Avocent - Cybex Secure 8-port DVI-I KVM Switch w/audio and DPP - Model SC 880DD, Part number 520-961-501, Ver. 33333-C3C3;
- Avocent - Cybex Secure 4-port DVI-I Dual-Head KVM Switch w/audio and DPP - Model SC 845DD, Part number 520-958-501, Ver. *33333-C3C3;*
- Avocent - Cybex Secure 8-port DVI-I Dual-Head KVM Switch w/audio and DPP - Model SC 885DD, Part number 520-958-501, Ver. 33303-C3C3;
- Avocent - Cybex Secure 16-port DVI-I KVM Switch w/audio and DPP - Model SC 1016DD, Part number 520-963-501, Ver. 33333-C3C3;
- Avocent - Cybex Secure 4-port KM Switch w/audio - Model SC 840KM, Part number 520-926-501, Ver. 33303-C3C3;
- Avocent - Cybex Secure 4-port KM Switch w/audio and DPP - Model SC 840KMP, Part number 520-959-501, Ver. 33333-C3C3; or
- Avocent - Cybex Secure 8-port KM Switch w/audio - Model SC 880KM, Part number 520-927-501, Ver. 33303-C3C3.

The Remote Desktop Controller (RDC) Model ESC 100, Part number 520-944-501, Ver. 4-A3 was evaluated on all models.

The publications in section 9 of this report describe the procedures necessary to install and operate Avocent KVM Switch in its evaluated configuration.

9 Documentation

The Avocent Corporation (Emerson) documents provided to the consumer are as follows:

a. User Manual Avocent Cybex Secure DisplayPort KVM, Rev. 1.1
b. User Manual Avocent Cybex Secure Windowing KVM, Rev. 1.1
c. User Manual Avocent Cybex Secure KVM Mini-Matrix, Rev. 1.1
d. User Manual Avocent Cybex Secure KM Switch, Rev. 1.1
e. User Manual Avocent Cybex Secure DVI-I KVM Dual-Head Switch with Audio, Rev.1.1
f. User Manual Avocent Cybex Secure Windowing KVM, Rev. 1.1
g. User Manual Avocent Cybex Secure KM Switch, Rev. 1.1
h. User Manual Avocent Cybex Secure KM Switch w/Audio and DPP, Rev. 1.1
i. User Manual Avocent Cybex Secure DVI-I KVM Switch, Rev. 1.1
j. SC840D/SC840DD 4-Port DVI-I Secure KVM Switch User Manual, Rev. 1.1
k. Avocent Cybex 8-Port DVI-I Secure KVM Switch User Manual, Rev. 1.1
l. SC840H/SC845H 4-Port Single/Dual Head HDMI Secure KVM Switch User Manual, Rev. 1.1
m. User Manual Avocent Cybex Secure Remote Desktop Controller (RDC), Rev. 1.1
n. Avocent Cybex Secure 2 port DVI-D/HDMI/DP KVM Switch User Manual, Rev. 1.1
o. User Manual Avocent Cybex Secure DVI-I KVM Dual-Head Switch with Audio, Rev.1.1
p. Avocent Cybex 16-Port DVI-I Secure KVM Switch User Manual, Rev. 1.1
q. SC840HP/SC845HP 4-Port Single/Dual Head HDMI Secure KVM Switch User Manual, Rev. 1.1

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Avocent KVM Switch, including the following areas:

Development: The evaluators analyzed the Avocent KVM Switch functional specification, design documentation, and a subset of the implementation representation; they determined that the design accurately describes the TOE security functionality (TSF) interfaces and the TSF subsystems and modules, and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the Avocent KVM Switch security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Avocent KVM Switch preparative user guidance and operational user guidance and determined that it sufficiently and

unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the Avocent KVM Switch configuration management system and associated documentation was performed. The evaluators found that the Avocent KVM Switch configuration items were clearly marked and could be modified and controlled by automated tools. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed and operated in accordance with the CM plan. The evaluators confirmed that the access control measures as described in the CM plan are effective in preventing unauthorised access to the configuration items.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Avocent KVM Switch during distribution to the consumer.

The evaluators examined the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the Avocent KVM Switch design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by Avocent Corporation (Emerson) for Avocent KVM Switch. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability Assessment: The evaluators conducted an independent vulnerability analysis of Avocent KVM Switch. Additionally, the evaluators conducted a review of public domain vulnerability databases and a focused search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to Avocent KVM Switch in its operational environment.

All these evaluation activities resulted in **PASS** verdicts.

11 ITS Product Testing

Testing at EAL 4 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[2].

The evaluators analyzed the developer's test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification, TOE design and security architecture description was complete.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of EWA-Canada test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Initialization: The objective of this test goal is to ensure that the system is initialized to a suitable state prior to independent testing.

c. Invalid USB Connection: The objective of this test goal is to verify that the Avocent KVM Switch will not allow access to a USB drive.

d. Default Settings: The objective of this test goal is to verify that the Avocent KVM Switch defaults to the host computer on start up.

11.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and a focused review of all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. Monitor for Information Leakage: The purpose of this test is to determine if the TOE is leaking any information that might be useful to an attacker;

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

b. Misuse by TOE User: The purpose of this test is to show that the TOE cannot be used to copy files to a USB drive or to move files from one host to another.

c. Misuse with USB Hub: The purpose of this test is to verify that a USB Hub may not be used with the Avocent KVM Switch.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

11.4 Conduct of Testing

Avocent KVM Switch was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at EWA-Canada. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that Avocent KVM Switch behaves as specified in its ST, functional specification, TOE design and security architecture description.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL4 + level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Evaluator Comments, Observations and Recommendations

Good security practices should be employed when fielding such a device. Ensure that only the recommended cables are used and that installation guidance is followed. All users of the TOE should be made aware that blinking LEDs are an indication that anti-tampering has been triggered.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme

Acronym/Abbreviation/ Initialization	Description
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
PSS	Peripheral Sharing Switch
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
USB	Universal Serial Bus

15 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. Peripheral Sharing Switch (PSS) Protection Profile for Human Interface Devices, version 2.1, 7 September 2010.

e. Avocent®-Cybex® Secure DVI KVM Switch, Secure KM Switch and Secure Windowing KVM, Security Target version 1.14, 16 July 2012

f. Evaluation Technical Report for EAL 4+ Common Criteria Evaluation of Avocent®-Cybex® Secure DVI KVM Switch, Secure KM Switch and Secure Windowing KVM, version 1.0, 16 July 2012.