Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2009/61

02 DEC 2009

Version 1.0

Amendment Record

Version	Date	Description
1.0	02 Dec 2009	Public release

Executive Summary

1 This report describes the findings of the IT security evaluation of Compucat Research Pty Ltd's Compucat Secure Optical Switch, to the Common Criteria (CC) evaluation assurance level EAL 7. The report concludes that the product has met the requirements of EAL 7 and that the evaluation was conducted in accordance with the relevant criteria and requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by the Australasian Information Security Evaluation Facility (AISEF) CSC Australia Ltd and was completed in February 2009.

2 The Compucat Secure Optical Switch is a hardware based tamper evident switching device that connects a single common port to any one of four selectable ports while maintaining isolation between the selectable ports within the body of the switch. The Compucat Secure Optical Switch, in both local and remote operation variants, is the Target of Evaluation (TOE).

3 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed, the Australasian Certification Authority (ACA) recommends the following:

a. Upon delivery of the TOE, in addition to the mechanisms described in Section 2.6.2, the customer should verify the integrity of the associated part numbers of the TOE by contacting the vendor;

b. As the physical protection of the TOE relies upon the integrity of its tamper evident seals, installers should record the seal integrity and locations upon delivery, and users and/or administrators should regularly examine the seals for evidence of tampering; and

c. The secure installation of the TOE should be accredited by an approved authority to an appropriate level for the data it is processing.

4 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 at Ref [1], and read this Certification Report prior to deciding whether to purchase the product.

5 The Common Criteria Mutual Recognition Arrangement recognises evaluation methodology to EAL 4. As this evaluation was Common Criteria v2.2 EAL 7, there was no internationally agreed methodology. The ACA provided EAL 7 methodology which the CSC AISEF applied to this evaluation.

Table of Contents

Chapter 1 - Introduction

1.1 Overview

6 This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

7 The purpose of this Certification Report is to:

a. report the certification of results of the IT security evaluation of the TOE, the Compucat Secure Optical Switch, against the requirements of the Common Criteria (CC) evaluation assurance level EAL 7, and

b. provide a source of detailed security information about the TOE for any interested parties.

8 This report should be read in conjunction with the TOE's Security Target (Ref [1]) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

9 Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 2.6.1 Evaluated Configuration.

Table 1: Identification Information

Item	**Identifier**
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Compucat Secure Optical Switch
Hardware Version	P/N 1105-0062-04 (local operation) and P/N 1105-0067-04 (remote version)
Security Target	Secure Optical Switch Security Target, P/N 2066-0012-05, Version 01, February 2008
Evaluation Level	EAL 7
Evaluation Technical Report	Secure Optical Switch (T0057), Evaluation Technical Report CSC-EFC-T0057-ETR, Version 2.0, 18 Nov 2009
Criteria	CC Version 2.2, Revision 256, CCIMB-2004-01-001, January 2004, with interpretations as of 22 April 2005
Methodology	CEM Version 2.2, Revision 256, CCIMB-2004-01-004, January

	2004, with interpretations as of 22 April 2005; and CEM EAL 7, CC Version 2.2, Defence Signals Directorate, Australasian Information Security Evaluation Program, 2005 and 2006.
Conformance	CC Part 2 Conformant CC Part 3 Conformant
Developer	Compucat Research Pty Ltd, 14 Wales Street, BELCONNEN, ACT 2617, Australia. http://www.compucat.com.au
Evaluation Facility	CSC Australia Pty Ltd, 217 Northbourne Avenue, TURNER ACT 2612, Australia. http://www.csc.com/commoncriteria

Chapter 2 - Target of Evaluation

2.1 Overview

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

2.2 Description of the TOE

11 The TOE is the Compucat Secure Optical Switch (SOS) developed by Compucat Research Pty Ltd. It is a hardware based tamper evident fibre-optic switching device that connects a single common port to any one of four selectable ports while maintaining isolation between the selectable ports within the body of the switch.

12 There are two variants of the SOS; the local operation option has a selector dial incorporated onto the unit; while the SOS remote operation option has connectors to allow remote selection and optical feedback of the selected switch position.

13 The TOE operates logically as a trusted switching device that connects a common port to any one of four selectable ports. The security functions claimed are:

a. The common port can be connected to only one selectable port at any one time;

b. The selectable ports can never be connected to each other via the TOE;

c. Indication is provided by the TOE unequivocally confirming to which selectable port the common port is connected; and

d. Tamper evidence of the physical case of the TOE.

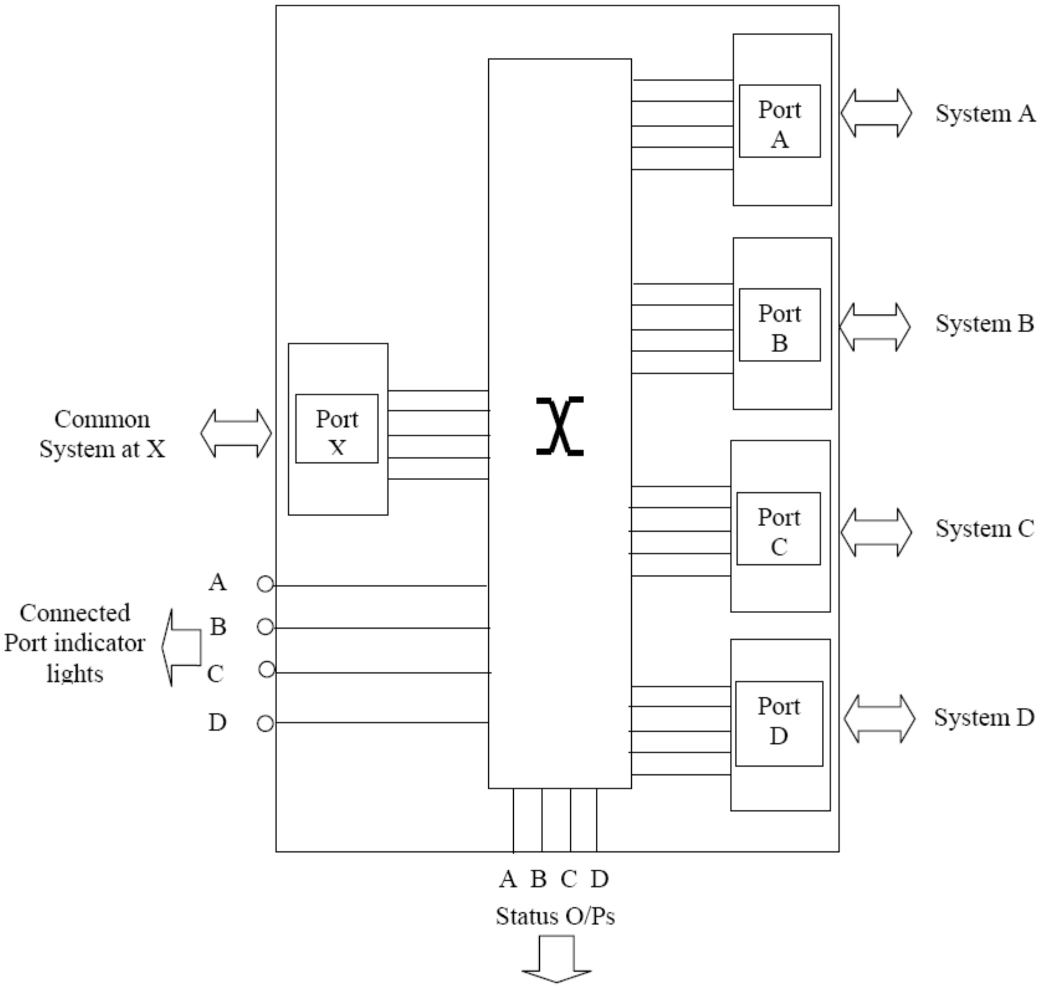

Figure 1 - Conceptual diagram of the Secure Optical Switch

2.3 Security Policy

14 The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. The TOE enforces the Single Connection Policy.

15 The TSP is implemented by the SFR’s listed below:

2.3.1 FDP_IFC.1

16 This policy identifies the name and information flow aspects in the scope of the Single Connection Policy switch stating the TOE has five information flow controlled ports in total. Common port X and selectable ports A, B, C, and D.

2.3.2 FDP_IFF.1

17 This policy defines the four possible valid connection states as common port X connected to either port A or B or C or D, stipulating that ports A, B, C and D cannot interconnect at any time. The policy also states that when port A, B, C or D has been selected the visual indication in the form of the LED also corresponds with the port selected.

2.3.3 FMT_MSA.1 and FMT_SMF.1

18 These policies state that users can use the selection input to manually select which port of A, B, C, or D that they want connected to common port X. In the normal mode of operation the user selection is directly reflected in the connection and indicator state of the TOE.

2.3.4 FPT_PHP.1

19 This policy states that the tamper evidence seal can only be in one of two states; intact or broken. If the seal is broken the TOE may be compromised and should no longer be trusted.

20 Each Security Functional Requirement (SFR) from the Security Target was modelled using formal Z schemas. In addition the possible error states were also modelled as separate schemas.

2.4 TOE Architecture

21 The TOE consists of the following major architectural components:

a. **BARS**: This subsystem provides the Opto-mechanical Switch function which selectively connects groups of optical fibres. The Opto-mechanical Switch ensures that just one selectable group of optical fibres can be connected to the corresponding fibres of the common port at any one time. The Switch Position Visual Indicator and the Switch Position Status Output are altered by this subsystem to provide unambiguous feedback of the selected port.

b. **SERVO**: This subsystem moves the sliding bar in the BARS subsystem to the required switch position to match the selection input by the user.

c. **ILOI**: This subsystem converts a power input provided by the POWERREG subsystem into two light sources required to output the TOE connectivity status via the Switch Position Visual Indicator and the Switch Position Status Output. These light sources are provided to the BARS subsystem, which in turn provides the output to the user of the selected port.

d. **POWERREG**: This subsystem provides power to the SERVO and ILOI subsystem – it does not directly contribute to any security function.

2.5 Clarification of Scope

22 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]).

2.5.1 Evaluated Functionality

23 The TOE provides the following evaluated security functionality:

a. Opto-mechanical switch;

b. Switch Position Visual Indication;

c. Switch Position Status Output; and

d. Tamper Evident case

2.5.2 Non-evaluated Functionality and Services

24 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 (ISM) (Ref [2]) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

25 Potential users should carefully consider the scope of the TOE. It has been assumed that devices connected to the TOE do not introduce security vulnerabilities. Also, no potential security features of these peripherals have been included within the evaluation. The TOE, by itself, has not had any functionality evaluated for securing connections between networks or peripherals of different security classifications, or for enforcing uni-directional data flow. If those functions are required then products which have been specifically evaluated for that security functionality should be employed.

2.6 Usage

2.6.1 Evaluated Configuration

26 This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in these defined evaluated configurations. Australian Government users should refer to the ISM (Ref [2]) to ensure that configurations meet the minimum Australian Government policy requirements. New Zealand Government users should consult the GCSB.

27 The TOE is the following hardware:

a. P/N 1105-0062-04 (local operation version); and

b. P/N 1105-0067-04 (remote operation version).

28 The TOE is a self contained hardware switching device which is available in two different versions – one that has a local dial to select ports and which has local switch position indication, and one that is remotely controlled and provides remote switch position indication.

2.6.2 Delivery procedures

29 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated product. The SOS is hardware that is sealed in its own case with tamper evident seals and delivered in one of the five methods:

a. Delivery and installation on site by a cleared Compucat technician;

b. Delivery to site by a cleared Compucat staff member;

c. Delivery via the Commonwealth safe hand system;

d. Delivery by safe hand courier; or

e. Customer safe hand collection.

30 The user guide provides advice on checking the security seals to ensure that the product has not been tampered with during delivery.

2.6.3 Determining the Evaluated Configuration

31 The User Guide lists the TOE’s identification part numbers. Each version of the TOE has a unique Compucat part number displayed on the case, with the final digits being the version number.

32 The customer should check that the TOE matches the identification provided on the despatch document and the evaluated part numbers in the Security Target.

2.6.4 Documentation

33 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:

a. User and Administrator Guide (Ref [3]).

2.6.5 Secure Usage

34 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.

35 The following assumptions were made:

a. The TOE should be in a physically secure environment that at least corresponds to the level of protection of the highest security level of data accessible through it.

b. The cabling connections of the TOE are complex and security critical. Installation and testing of the TOE should be restricted to suitably trained and cleared personnel.

c. System administrators are assumed to be cleared and suitably trained to check the operational status of the switch. Where cabling configurations are to be changed this should be undertaken by a suitable trained, cleared and authorised technician.

d. In addition to installer and administrator training, users must be trained in the secure use of the switch and to recognise indications of switch failure or improper operation.

e. All personnel should be cleared to at least the highest level of data that they are capable of accessing within the switch's environment.

2.6.6 Error Conditions

36 The TOE may enter possible error states. These are:

a. the TOE has jammed between ports;

b. there is an indicator light failure;

c. the TOE is transiting to a new selected connection; and

d. the TOE is powered down.

37 If any of the above conditions occur then the TOE has entered an untrusted state and the true connection status of the TOE cannot be verified by the operator. Guidance (Ref [3]) is provided to inform users how to identify when the TOE is in an untrusted state and how to handle the TOE when it is in that state.

Chapter 3 - Evaluation

3.1 Overview

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

3.2 Evaluation Procedures

39 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation (Refs [4], [5] and [6]). The methodology

used is described in the Common Methodology for Information Technology Security Evaluation (CEM) (Ref [7]). The evaluation was also carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [8], [9], [10] and [11]). In the absence of internationally agreed methodology above EAL 4, AISEP-developed methodology was used for this EAL 7 evaluation (Ref [12]). The conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [13]) were also upheld.

3.3 Functional Testing

40 EAL 7 analysis is supported by

a. independent testing of the TOE security functions,

b. evidence of developer testing based on the functional specification high-level design,

c. low-level design and implementation representation,

d. complete independent confirmation of the developer results,

e. strength of function analysis,

f. evidence of a developer search for vulnerabilities, and

g. an independent vulnerability analysis demonstrating resistance to penetration attackers with a high attack potential.

41 The analysis also includes validation of the developer's systematic covert channel analysis.

3.4 Penetration Testing

42 The developer performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. Based on this analysis the evaluators developed and executed penetration tests.

43 Even though the security target assumes physical security of the TOE, the evaluators did not take this into consideration for a physical tamper test. This allowed the evaluators to fully test the tamper evident security measures used by the TOE. Testing identified a case lid vulnerability which was corrected.

Chapter 4 - Certification

4.1 Overview

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

4.2 Certification Result

45 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report (Ref [14]), the Australasian Certification Authority certifies the evaluation of the Compucat Secure Optical Switch performed by the Australasian Information Security Evaluation Facility, CSC Australia. The evaluation was conducted concurrently with the development of the TOE.

46 CSC Australia has found that Compucat Secure Optical Switch upholds the claims made in the Security Target (Ref [1]) and has met the requirements of Common Criteria evaluation assurance level EAL 7.

47 The Common Criteria Mutual Recognition Arrangement only recognises evaluation methodology to EAL 4. As this evaluation was for Common Criteria v2.2 EAL 7, there was no internationally agreed methodology. The ACA provided EAL 7 methodology (Ref [12]) which the AISEF applied to this evaluation.

48 Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Assurance Level Information

49 EAL 7 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a structured presentation of the implementation, to understand the security behaviour. Assurance is additionally gained through a formal model of the TOE security policy, a formal presentation of the functional specification and high-level design, a semiformal presentation of the low-level design, and formal and semiformal demonstration of correspondence between them, as appropriate. A modular, layered and simple TOE design is also required.

50 EAL 7 also provides assurance through the use of a structured development process, development environment controls, comprehensive TOE configuration management (including complete automation of that process) and evidence of secure delivery procedures.

4.4 Recommendations

51 Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to the ISM (Ref [2]) and New Zealand Government users should consult the GCSB.

52 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Ref [3]), the ACA also recommends the following:

a. Upon delivery of the TOE, in addition to the mechanisms described in Section 2.6.2, the customer should verify the integrity of the associated part numbers of the TOE by contacting the vendor;

b. As the physical protection of the TOE relies upon the integrity of its tamper evident seals, installers should record the seal integrity and locations upon delivery, and users and/or administrators should regularly examine the seals for evidence of tampering; and

c. The secure installation of the TOE should be accredited by an approved authority to an appropriate level for the data it is processing.

Annex A - References and Abbreviations

A.1 References

[1] Secure Optical Switch Security Target, P/N 2066-0012-05, Version 01, February 2008

[2] Australian Government Information Security Manual (ISM), September 2009, Defence Signals Directorate, (available at www.dsd.gov.au).

[3] Secure Optical Switch USER and ADMINISTRATOR GUIDE, P/N 2066-0021-04, Compucat, October 2008.

[4] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 2.2 Revision 256, January 2004, CCIMB-2004-01-001

[5] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 2.2, January 2004, CCIMB-2004-01-002

[6] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 2.2 Revision 256, January 2004, CCIMB-2004-01-003

[7] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.2 Revision 256, January 2004, CCIMB-2004-01-004

[8] AISEP Publication No. 1 – Program Policy, AP 1, Version 3.1, 29 September 2006, Defence Signals Directorate.

[9] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.0, 21 February 2006, Defence Signals Directorate.

[10] AISEP Publication No. 3 – Evaluator Guidance, AP 3. Version 3.1, 29 September 2006, Defence Signals Directorate

[11] AISEP Publication No. 4 – Sponsor and Consumer Guidance, AP 4. Version 3.1, 29 September 2006, Defence Signals Directorate

[12] AISEP Publications, CC v2.2 EAL 7 Common Evaluation Methodology http://www.dsd.gov.au/infosec/evaluation_services/epl/aisep_doc_guide.html

[13] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000

[14] Evaluation Technical Report, CSC-EFC-T0057-ETR, v2.0, 18 Nov 2009

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program http://www.dsd.gov.au/infosec/evaluation_services/aisep_pages/aisep.html
CC	Common Criteria http://www.commoncriteriaportal.org
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate http://www.dsd.gov.au
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau http://www.gcsb.govt.nz
ISM	Australian Government Information Security Manual
LED	Light Emitting Diode
PP	Protection Profile
SCEC	Security Construction and Equipment Committee http://www.scec.gov.au/
SFP	Security Function Policy
SFR	Security Functional Requirements
SOS	Secure Optical Switch
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy