C032 Certification Report
Ornet Neuron Version 1.2.2

File name: ISCB-5-RPT-C032-CR-v1a
Version: v1a
Date of document: 26 March 2012
Document classification: PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 8, Block A
Mines Waterfront Business Park
No 3 Jalan Tasik, The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.
T +603 8946 0999
F +603 8946 0888
www.cybersecurity.my

C032 Certification Report

Ornet Neuron Version 1.2.2

26 March 2012

ISCB Department

CyberSecurity Malaysia

Level 8, Block A, Mines Waterfront Business Park,

No 3 Jalan Tasik, The Mines Resort City

43300 Seri Kembangan, Selangor, Malaysia

Tel: +603 8946 0999 Fax: +603 8946 0888

http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C032 Certification Report - Ornet Neuron Version 1.2.2
DOCUMENT REFERENCE:	ISCB-5-RPT-C032-CR-v1a
ISSUE:	v1a
DATE:	26 March 2012

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 8, Block A,

Mines Waterfront Business Park,

No 3 JalanTasik, The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

Printed in Malaysia

Forward

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB 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 26 March 2012, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement at www.commoncriteriaportal.org).

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 3 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 3 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
v1	13 March 2012	All	Final Released
v1a	26 March 2012	Page iv	Add the date of the certificate.

Executive Summary

The Ornet Neuron version 1.2.2 (hereafter referred as Ornet Neuron) from Ornet Solutions Sdn Bhd is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 1 evaluation.

Ornet Neuron is a web based application for user to monitor the performance of machines used in semiconductor and electronic manufacturing factories.

The TOE is software that comprises of five modules:

- Failure Mode and Effect Analysis (FMEA),
- Machine Performance Analyzer (MPA),
- Statistical Process Control (SPC),
- Tool Life Scheduling (TLS),
- Reject Analysis (RA).

The functions of the TOE that are within the scope of evaluation covering the access control functions that permits a user to access the machine information, identification and authentication functions for user to identify and authenticate themselves before performing any action, and security management which includes user management and machine management.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for Ornet Neuron, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with substances that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the IT security evaluation of Ornet Neuron to the Common Criteria (CC) evaluation assurance level EAL1. The report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]). The evaluation was performed by the Stratsec.net Sdn Bhd (Stratsec) Security Evaluation Facility (Stratsec MySEF) and completed on 27 February 2012.

The Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the Ornet Neuron evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and the product will be listed on the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement at www.commoncriteriaportal.org).

It is the responsibility of the user to ensure that the Ornet Neuron meets their requirements and security needs. It is recommended that a potential user of the Ornet

Neuron to refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE), Ornet Neuron version 1.2.2 (hereafter referred as Ornet Neuron) is a web based application that allows users to monitor the performance of machines used in semiconductor and electronic manufacturing factories. The TOE is software that comprises of:

a) Failure Mode and Effect Analysis (FMEA), a module designed to send and receive failure mode immediately and screened in the spreadsheet.

b) Machine Performance Analyzer (MPA), a module where user used to view reports according to the search selection using the MPA interface.

c) Statistical Process Control (SPC), is intended to help user to do data entry and generate report based on their entry.

d) Tool Life Scheduling (TLS), comes with various maintenance tasks such as preventive maintenance, tasks scheduling, tasks reminder, shutdown planning. There are also other tasks included such as inspection, lubrication, parts change and servicing.

e) Reject Analysis (RA), is a module designed to track and monitor rejects in the production area. User can do data entry and generate reports.

2 The Evaluated security functionalities for TOE includes:

a) **Access control -** The TOE manages access control based on user IDs, user roles and access control lists.

b) **Identification and Authentication** – The TOE requires that each user is successfully identified (User ID) and authenticated (password) before they are allowed to perform any action on the TOE.

c) **Security Management** - The TOE provides functions that allow management of the TOE and its security functions.

1.2 TOE Identification

3 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C032
TOE Name	Ornet Neuron
TOE Version	Version 1.2.2
Security Target Title	Ornet Neuron Security Target

Security Target Version	Version 1.1
Security Target Date	16 February 2012
Assurance Level	Evaluation Assurance Level 1 (EAL1)
Criteria	Common Criteria for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL1
Sponsor and Developer	Ornet Solutions Sdn Bhd, Suite 19, Incubator Wing, 1st Floor, Techno Centre, Kulim Hi-Tech Park, 09000 Kulim, Kedah, MALAYSIA Tel: 04-403 6300
Evaluation Facility	Stratsec MySEF

1.3 Security Policy

4 Ornet Neuron implements Access Control Policy on protected information where user need to be authenticated and identified before being able to access the protected information.

5 The details of the security policy are described in Section 5.1 of the Security Target (Ref [6]).

1.4 TOE Architecture

6 Ornet Neuron includes both logical and physical boundaries which are described in Section 1.3.3 and Section 1.4 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

7 The TOE security functions comprises of the following:

a) **Access control -** The TOE manages access control based on user IDs, user roles and access control lists. The TOE maintains access control lists for each

object. Each ACL maps users and roles to the modules and functions that they are permitted to perform.

b) **Identification and authentication -** The TOE requires that each user is successfully identified and authenticated before any interaction with the functionality of the TOE is permitted.

c) **Security Management** - The TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user.

1.4.2 Physical Boundaries

8 Figure 1 below describes the physical scope of Ornet Neuron;

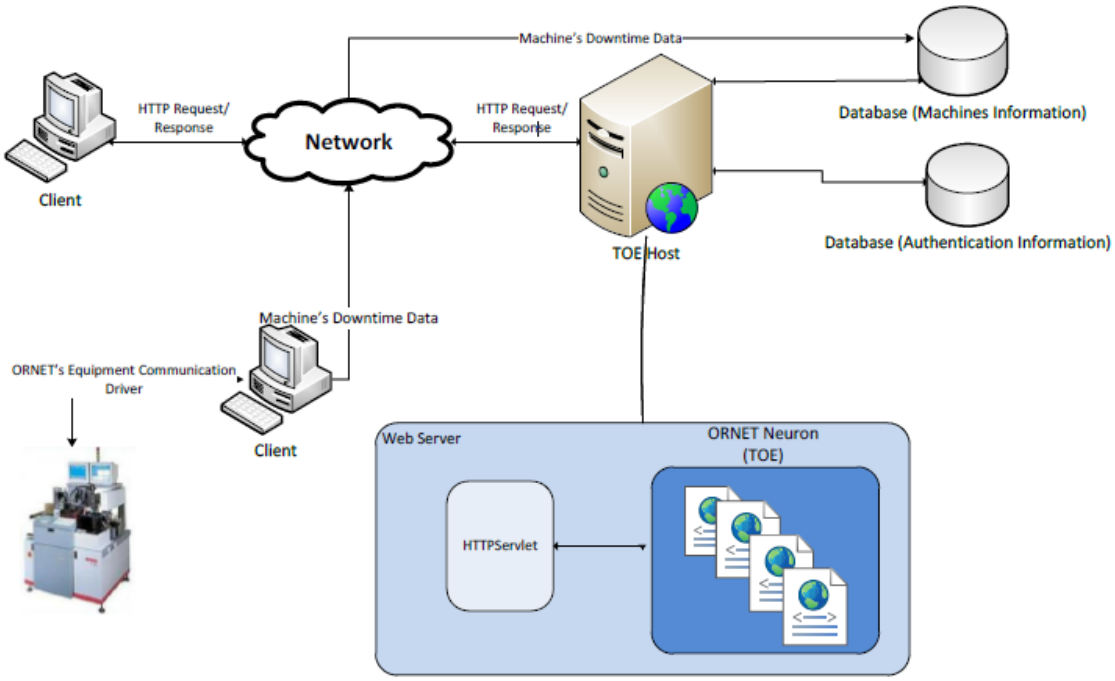

Figure 1: TOE Physical Scope

9 Physically, the TOE is a web application hosted in a web server. Therefore the TOE requires separate server for each of the system and a client machine with 3.0GHz processor, operating system, database and other supporting softwares as described in Section 1.3.4 of the Security Target (Ref [6]).

10 The Security Target assumes that environment provides appropriate physical security for the TOE. This would restrict access to the TOE directly.

1.5 Clarification of Scope

11 The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, personnel and communication security in accordance with administrator guidance that is supplied with the product.

12 Section 1.4.1 of this document described the scope of the evaluation. The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality:

a) **Access Control** – Access to the TOE and TOE protected resource (machine information) is restricted to user that has permission and access rights to that information only by identifying the user roles. The access control and security roles described in more detail in Section 5.1.1 of the Security Target (Ref [6]). There are seven users maintained by the TOE: Administrator, User Admin, Machine Admin, Reset Password, Data Entry, View Reports, and Standard Control Limit. Each type of users will have different access rights to a protected resource.

b) **Identification and Authentication** – All users including administrator must be identified and authenticated before being able to perform any action. TOE will checks the credentials of the user upon the login page against the information stored in the database including user ID and password. Described in more detail in Section 5.1.2 of the Security Target (Ref [6]).

c) **Security Management** – Authorized Administrator and User Admin can query, delete, create, modify user account and modify the access control list by modifying the user to roles mapping. While authorized roles including Administrator, User Admin and Reset Password are allow to modify user password. Security Management described in more detail in Section 5.1.3 of the Security Target (Ref [6]).

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

14 Functions and services which are not included as part of the evaluated configuration, but these IT environment are required to ensure that the TOE perform in its intended operations, are as follows:

a) A Hardware Server;

b) An Operating System on which the TOE is installed on;

c) A Database Software on which the TOE is dependent on as its database;

d) Other supporting software;

i) Microsoft IIS version 5.1.

ii) Microsoft .NET framework 2.0.

iii) Microsoft .NET framework 3.5.

iv) Internet Explorer version 7.0.

v) Internet Browser.

1.6 Assumptions

15 There is no assumption for the TOE defined in the Security Target (Ref [6]).

1.7 Evaluated Configuration

16 This section describes the configurations of the TOE that are included within the scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in the defined evaluated configuration according to the documented preparative user guidance (Ref 22a)).

17 The TOE is delivered to the customer by the developer's staff only. The developer's staff then install the TOE and make changes to the configuration based on preparative user guidance (Ref 22a)) as following:

a) Installation and configuration of Ornet Neuron.

b) Configuration of UDL.

c) URL connection testing.

1.8 Delivery Procedures

18 Ornet Neuron is delivered to the user by the developer's administrator staff.

19 However, for this EAL1 evaluation, TOE Delivery (ALC_DEL) is not included in the scope of the evaluation. Thus, developer did not provide any documentation on TOE delivery and the evaluators did not verify any TOE delivery process.

1.9 Documentation

20 To ensure continued secure usage of the product, it is important that the Ornet Neuron is used in accordance with guidance documentation.

21 The following documentation is provided by the developer to the end user as guidance to ensure secure operation of the product:

a) TLS User Guide, version 1.2, 8 December 2010.

b) Admin User Guide, version 1.0, 9 December 2010.

c) CPAC User Guide, version 1.1, 8 December 2010.

d) FMEA User Guide, version 1.2, 8 December 2010.

e) MPA User Guide, version 1.1, 8 December 2010.

f) RA User Guide, version 1.2, 8 December 2010.

g) SPC User Guide, version 1.2, 8 December 2010.

22 The following documentation is used by the developer's authorised personnel as guidance to ensure secure installation of the product:

a) ORNET Neuron WebSetup User Guide and UDL, version 1.2, 8 December 2010.

2 Evaluation

23 The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 3 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 3 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 1 (EAL1). The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [5]).

2.1 Evaluation Analysis Activities

24 The evaluation activities involved a structured evaluation of Ornet Neuron, including the following components:

2.1.1 Life-cycle support

25 An analysis of the Ornet Neuron configuration management system and associated documentation was performed. The evaluators confirmed that the configuration list which includes the TOE and the evaluation evidence were clearly and uniquely labelled.

2.1.2 Development

26 The evaluators analysed the Ornet Neuron functional specification; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces (TSFIs), and how the TSF implements the security functional requirements (SFRs).

2.1.3 Guidance documents

27 The evaluators examined the Ornet Neuron preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

2.1.4 IT Product Testing

28 Testing at EAL1 consists of performing independent function test, and performing penetration tests. The Ornet Neuron testing was conducted at Stratsec MySEF lab in Plaza Sentral, Kuala Lumpur. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Reports.

2.1.4.1 Independent Functional Testing

29 At EAL1, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining functional and guidance documentation, and creating test cases to verify the behaviour of the TOE.

30 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The result of the independent tests developed and performed by the evaluators to verify the TOE functionality are as follows:

Table 2: Independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
To test the [**Access Control SFP**] on [**Subjects:** **a) HTTP request on behalf of users** **Objects:** **a) Protected resources (machine information)** **Operations: Viewing, modification of machine information**]	FDP_ACC.1 : Subset access control	User Interface	**PASS**. Result as expected.
To test the enforcement of [**Access Control SFP**] to objects based on the following: [**Subject attribute:** **a) ID of the user** **b) corresponding user role** **Object attributes: Access Control List**] To test the operation among controlled subjects and controlled objects is allowed based on rules below: [**The operation is allowed, if:** **a) The Access Control List for an object permits the user ID to access that object; OR** **b) The Access Control List for an object permits the User Role to**	FDP_ACF.1 : Security attribute based access control	User Interface Database Interface	**PASS**. Result as expected.

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
access that Object.]			
To test that user is properly authenticate before continue with other action	FIA_UAU.2 : User authentication before any action	User Interface Database Interface and Audit log review functions	**PASS**. Result as expected.
To test that user is properly identified before continue with other action.	FIA_UID.2 : User identification before any action	User Interface Database Interface	**PASS**. Result as expected.
Run test to ensure that only [**the Administrator role, User Admin Role**] is having the [***write or delete***] security attributes [**that map user IDs to roles to only the users that are mapped**]	FMT_MSA.1a : Management of security attributes	User Interface	**PASS**. Result as expected.
The TSF shall enforce the [**Access Control SFP**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP. The TSF shall allow the [**Administrator, User Admin**] to specify alternative initial values to override the default values when an object or information is created.	FMT_MSA.3.1 and FMT_MSA.3.2: Static attribute initialisation	Database Interface	**PASS**. Result as expected.
To test the TOE ability to restrict the function of [***query, modify, delete, clear***[**Create]** which map the users to roles and user account to [**Administrator and User Admin Role**] To test that only [**the Administrator role, User Admin Role and the Reset Password Role**] have ability to [***modify***] the [**User Password**]	FMT_MTD.1b : Management of TSF data	User Interface Database Interface	**PASS**. Result as expected.
To test the management functions	FMT_SMF.1 :	User Interface	**PASS**. Result as

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
of TOE: [**a) mapping user IDs to roles** **b) creation of users with default passwords** **c) deletion of users** **d) changing of passwords** **e) management of Access Control lists** **f) manage machine information** **g) reset password**]	Specification of Management Functions	Database Interface	expected.
Run test to ensure the TOE maintain the roles of [**Administrator, User Admin, Machine Admin, Reset Password, Data Entry, View Reports and Standard Control Limit roles**]. To test that the TOE shall be able to associate users with roles.	FMT_SMR.1 : Security roles	User Interface Database Interface	**PASS**. Result as expected.

31 All tests performed by the evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.2 Penetration Testing

32 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, and functional specification.

33 From the vulnerability analysis, the evaluators conducted penetration testing to determine whether potential vulnerabilities could be exploited in the intended operating environment of the TOE, to attack performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE;

d) Window of opportunity; and

e) IT hardware/software or other requirement required for exploitation.

34 The penetration tests focused on:

a) Generic vulnerabilities;

b) Bypassing;

c) Tampering; and

d) Direct attacks.

35 The results of the penetration testing note that there is no exploitable vulnerability and/or residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment.

2.1.4.3 Testing Results

36 Tests conducted for the Ornet Neuron produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

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

3 Result of the Evaluation

38 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of Ornet Neuron performed by the Stratsec MySEF.

39 Stratsec MySEF found that Ornet Neuron upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) assurance level EAL1.

40 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities undiscovered in its claimed security functionality. This risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

41 EAL1 provides a basic level of assurance by a limited Security Target and an analysis of the security functions in that Security Target, using a functional and interface specification and guidance documentation, to understand the security behaviour.

42 The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TOE security functions.

43 EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.

44 This EAL provides a meaningful increase in assurance over unevaluated IT.

3.2 Recommendation

45 In addition to ensure secure usage of the product, below are additional recommendations for Ornet Neuron consumers:

a) Review the intended operational environment and ensure that all elements are suitably maintained and addressed. It is important the following be continually maintained:

   i) The servers that host the web and database servers are hosted in a secure operating facility with restricted physical access with non-shared hardware.

   ii) The databases in the TOE environment have been correctly configured according to the principle of least privilege.

   iii) There is appropriate network layer protection in place that only permits access through required ports for external users to access the web-server.

   iv) The underlying operating system, web-server, application server and DBMS are patched and hardened to protect against known vulnerabilities and security configuration issues.

v) That secure coding principles are always followed so that injection and scripting vulnerabilities are not introduced into the operational environment.

b) The users of the TOE should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.

c) Implement an encrypted communication layer (https) for all authentications and sensitive data transfer between client and server. Secure communication is important since it can nearly avoid the data from being sniffed by unauthorized parties.

d) Ensure the TOE is to be located in a physically secured area.

e) Use the product only in its evaluated configuration.

f) Ensure the installation and configuration done by the developer follow the installation guidance document.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

[4] MyCC Scheme Policy (MyCC_P1), v1a, CyberSecurity Malaysia, December 2009.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1, December 2009.

[6] Ornet Neuron Security Target, Version 1.1, 16 February 2012

[7] Evaluation Technical Report EAL1 Evaluation of Ornet Neuron, Version 1.0, 27 February 2012

A.2 Terminology

A.2.1 Acronyms

Table 3: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology (ISO/IEC 18045)
IEC	International Electrotechnical Commission
ISCB	Information Security Certification Body
ISO	International Standards Organisation
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
SFP	Security Function Policy

Acronym	Expanded Term
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS ISO/IEC Guide 65
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.

Term	Definition and Source
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE

--- END OF DOCUMENT ---