CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI
Ministry of Science, Technology and Innovation

C026 Certification Report
E-Jari v 4.0

File name: ISCB-5-RPT-C026-CR-v1a
Version: v1a
Date of document: 16 May 2011
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

Securing Our Cyberspace

C026 Certification Report
E-Jari v 4.0

16 May 2011

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:	C026 Certification Report - E-Jari v 4.0
DOCUMENT REFERENCE:	ISCB-5-RPT-C026-CR-v1a
ISSUE:	v1a
DATE:	16 May 2011

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 16 May 2011, 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.

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	29 April 2011	All	Final Released.
v1a	16 May 2011	Page iv	Add the date of the certificate.

Executive Summary

E-Jari v 4.0 from Neural Services Sdn Bhd is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 1 evaluation.

The TOE comprises of:

- E-Jari v 4.0, is the software identifier, that represents the firmware part for this TOE; and
- NM4000, is the hardware identifier, that represents the hardware part of this TOE.

E-Jari v 4.0 is the biometric verification system that either verifies or rejects the claimed identity of a human being using unique characteristics of his body: his fingerprint. The scope of the evaluation only covers the operation of E-Jari v 4.0 in a verification mode only: the system verifies whether, for a specific user ID, the fingerprint offered matches the fingerprint stored for the and only that user (commonly referred to as 1:1 matching). Although it can be used in stand-alone or network-integrated solutions, the evaluation only covers stand-alone operation only. Therefore, Biometric Identification (commonly referred to as 1:N matching) is not addressed by this Security Target (Ref [6]).

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for E-Jari v 4.0, the security 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 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 security evaluation of E-Jari v 4.0 to the Common Criteria (CC) evaluation assurance level EAL1. The report confirms that the product has met the target assurance level of EAL1 and 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 CyberSecurity Malaysia MySEF and was completed on 3 December 2010.

The Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the E-Jari v 4.0 evaluation meets all the conditions of the MyCC Scheme requirements and that the product will be listed on the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc.

It is the responsibility of the user to ensure that the E-Jari v 4.0 meets their requirements. It is recommended that a potential user of the E-Jari v 4.0 to refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase and deploy 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), E-Jari v 4.0, is biometric based identification and authentication system that implemented by the user as the access point to the portal. The portal means restricted area for the authorised user which assigned by the administrator. The TOE comprises of:

a) E-Jari v 4.0, is the software part of the TOE which controls the verification part and fingerprint matching; and

b) NM4000 is the hardware part of the TOE that capture the fingerprint template and extracting them for use to be compared between the enrolled minutiae from the flash memory.

1.2 TOE Identification

2 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	C026
TOE Name	E-Jari v 4.0
TOE Version	v 4.0
Security Target Title	Security Target for E-Jari version 4.0
Security Target Version	v0.24
Security Target Date	3 December 2010
Assurance Level	Evaluation Assurance Level 1 (EAL1)
Criteria	Common Criteria July 2009, Version 3.1, Revision 3
Methodology	Common Methodology for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL1
Sponsor and Developer	**Neural Services Sdn Bhd** No.4-3, Jalan 9/32A,Off Jalan Usahawan, Setapak, 43200 Kuala Lumpur

Evaluation Facility	CyberSecurity Malaysia MySEF

1.3 Security Policy

3 Based on the organisational security policy stated in Section 4.5 of the Security Target (Ref [6]), E-Jari v 4.0 :

a) shall meet recognise national and/or international criteria for its security relevant error rates (e.g. False Accept Rate (FAR) and False Rejection Rate (FRR)); and

b) repeated verification attempts using one or more claimed user IDs must be prevented from gaining access to the portal. The maximum number of unsuccessful verification attempts shall be limited.

4 E-Jari v 4.0 implements simple access control policy where successful verified users are granted entry by opening the portal (i.e. the door). This function is described further in Section 2.4.2 of the Security Target (Ref [6]). However this function is outside the scope of the evaluation.

1.4 TOE Architecture

5 E-Jari v 4.0 includes both logical and physical boundaries.

6 Figure 1 below describes the subsystem and components of E-Jari v 4.0 that comprise the TOE; the Main subsystem and the Sensor subsystem.

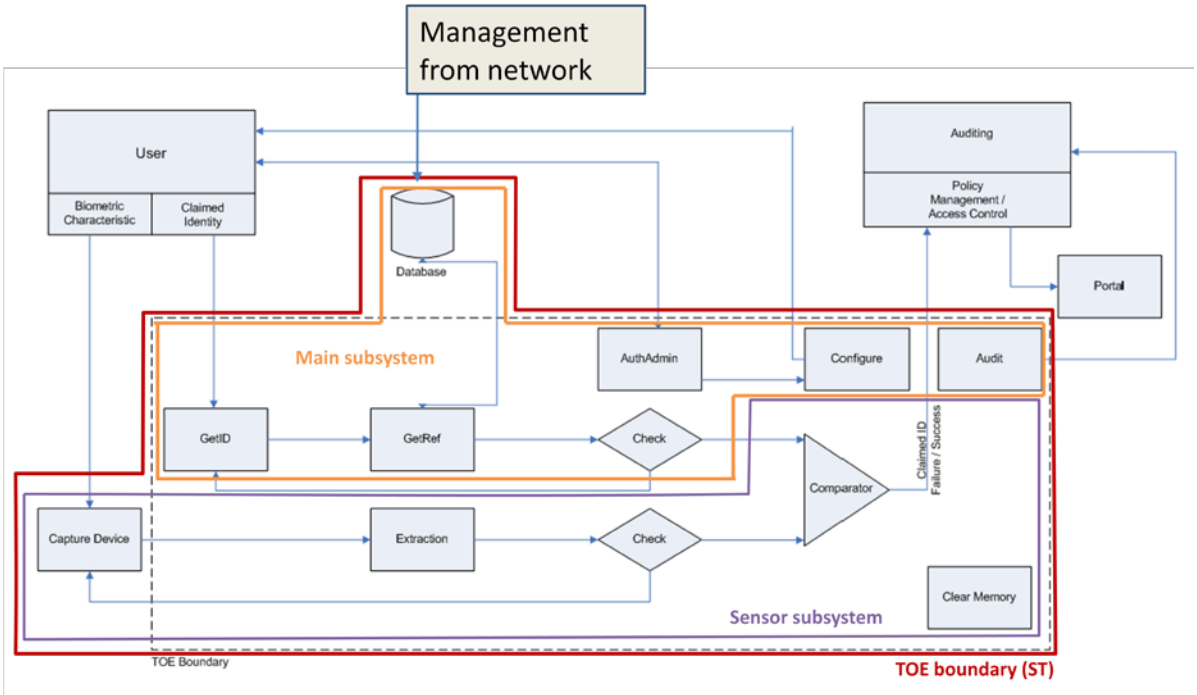

Figure 1: TOE Logical Scope

7 The TOE security subsystem comprise of the following:

a) **Main subsystem** – Provides the verification function of the TOE against the enrolled information in the flash memory which is call database. The database is used to store information of the biometric template during enrolment. The Main Subsystem consist of Database, GetID component, GetRef component, Check process, AuthAdmin component, Configure component and Audit component.

b) **Sensor subsystem** – Is the subsystem that captures the biometric minutiae from the human user extracting the information from the capacitance sensor and comparing them against the input from the Main Subsytem for verification checking. The Comparator then gives an output whether the minutia is success or fails against the claimed ID. This subsystem consists of Capture device, Extraction component, Check process, a Comparator and a Clear Memory component.

8 The TOE physical boundary is a mechanical moulding and electronic part of the E-Jari v 4.0 which makes up to be the NM4000. Physical diagram of the TOE can be referred to in section 2.4.1 “Physical boundary and features” of the Security Target (Ref [6]).

9 Additionally the E-Jari v 4.0 can also be connected to network connections for its connection features to work. However, it is out of the evaluation scope.

1.5 Clarification of Scope

10 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]). Based on Figure 1, the evaluated security functionalities include:

a) **Get ID**: The user's claimed identity is retrieved by reading the smartcard offered in the field of the contactless smartcard reader (part of the main subsystem). (Note that product allows entry of the normal user ID via the PIN pad, but this is outside the scope of the evaluation). The main subsystem also provides the PIN pad, display and status LEDs as the user visible interface, as well as audio feedback.

b) **GetRef**: The main subsystem is responsible for getting the stored (already enrolled) fingerprint reference related to a claimed user's identity.

c) **Extraction**: The sensor subsystem extracts the feature vector from the fingerprint sensor image. This feature vector allows robust and efficient verification in the checking phase, and effectively compressed the large sensor image to a much smaller feature vector.

d) **Check**: The integrity and authenticity of the fingerprint sensor image is ensured by including the sensor into the physical and logical boundary of the TOE. The integrity and authenticity of the stored fingerprint reference is also ensured by including the database into the physical and logical boundary of the TOE. The quality check on the live fingerprint offered is performed during the sensor module’s processing of the fingerprint sensor image. Insufficient quality will lead to a rejection in the verification.

e) **AuthAdmin**: Using the PIN pad of the main subsystem, the administrators can identify (by them using the PIN pad) and authenticate (by entering the correct PIN) themselves. Only after successful identification and authentication will the main subsystem allow access to the administration functionality (described directly below as “Configure”). This way it is ensured that only authenticated administrators are allowed to configure any of the security relevant settings of the TOE.

f) **Configure**: Using the PIN pad and display of the main subsystem, the administrator can set the TOE parameters (both security relevant and non-security relevant). The

threshold setting for the comparator component as well as the auditable events is fixed to a secure value to avoid potential mistakes in configuration.

g) **Comparator (also called Matcher)**: The sensor subsystem compares the enrolled fingerprint reference (retrieved via GetRef) with the offered fingerprint's feature vector (from Extraction). The sensor module internally verifies the two within a threshold that provides a False Acceptance Rate FAR of more than 1/100 and provides a fail/success value to the main subsystem. The main system optionally can perform time based access control but this is not in the scope of the evaluation. The result is provided to the environment and an audit event is generated. An "Exact match" comparison does not result in a positive verification as it may be a replay attempt and should be recorded in the audit log.

h) **Clear memory**: In order to protect against attacks on the raw fingerprint image data of the offered fingerprint, the sensor subsystem alone handles this data (hence its inclusion in the scope of the sensor module). The main subsystem does not access this data on the sensor subsystem. After the acquisition of the image, extraction and comparator actions, the fingerprint image data is therefore not accessible after de-allocation. Biometric reference data must be stored in the database for use in the system and is therefore exempt of this requirement.

i) **Audit**: Audit events are generated by the main subsystem and stored in its memory. It can be read via the management interface and the network interface, but this audit reviewing functionality is not in the scope of the evaluation.

j) **Capture device**: the fingerprint sensor is part of the sensor subsystem. It captures the fingerprint using a capacitive sensor array.

k) **Database**: Included in the TOE is the database used by the TOE to store the fingerprint reference of a user together with the user ID.

11 The evaluation scope does not cover:

a) **Enrolment process**: Function to 'learn' to verify the identity of each user based on their biometric characteristic (registering fingerprint user to TOE)

b) **Biometric Identification**: No claimed identity for the user. The system directly captures the biometric characteristic of a user and compares it to all biometric references in the database (commonly referred to as 1:N matching).

c) **Policy management/Access control**: Checking the user's rights and opening the portal if the user has sufficient privileges and was successfully verified by the TOE.

d) **Portal**: The physical or logical point beyond which information or assets are protected by a biometric system. Common deployment of the portal is the electronic lock of a door.

e) **Auditing**: The environment may provide additional audit functionalities and has to provide a mechanism for audit review of the TOE audit logs. The developer of the TOE has complementary network software to provide this functionality.

f) **Transmission / Storage**: The environment cares for a secure communication and storing where security relevant data is transferred to or from the TOE. This especially applies to the network connection and the connection to the portal.

12 The TOE can be used in stand-alone or network-integrated solutions. However, scope of evaluation covers only the stand-alone operation.

1.6 **Error! Reference source not found.**Assumptions

13 This section summarises the security aspects of the environment/configuration in which the IT product is intended to operate. Consumers should understand their own IT environments that required for secure operation of the E-Jari v 4.0 defined in subsequent sections and in the Security Target.

1.6.1 Usage assumptions

14 Assumptions for the TOE usage listed in the ST are:

a) Authorised administrator is well trained and non hostile. He reads and understands completely the content of the guidance documentation and adheres to it accordingly.

b) It is assumed that enrolment has already been performed and therefore, the biometric reference for each authorised user is assumed to be given. The generated reference is of sufficient quality and is linked to the correct user.

1.6.2 Environment assumptions

15 Assumptions for the TOE environment listed in the Security Target are:

a) The environment to where the TOE is installed is secure and is able to protect the TOE from an attacker presenting an imitated finger to the fingerprint sensor or to re-use the latent image on the fingerprint sensor surface, sufficient to withstand a real attacker up to moderate attack potential who uses a large amount of biometric characteristics and who really wants to get unauthorised access to the portal.

b) It is assumed that the environment protects the TOE sufficiently to prevent an attacker from presenting an imitated finger to the fingerprint sensor or to re-use the latent image on the fingerprint sensor surface, sufficient to withstand a real attacker up to moderate attack potential who uses a large amount of biometric characteristics and who really wants to get unauthorised access to the portal.

c) The fall-back mechanism for the biometric verification system is available that reaches at least the same level of security as the biometric verification system does. This fall-back system is used in cases where an authorised user is rejected by the biometric verification system (False Rejection).

d) It is assumed, that necessary TOE operating equipment and adequate infrastructure is available (e.g.: operating system, database, LAN, public telephone, and guardian). Specifically the following things are assumed:

- It is assumed that the direct environment of the TOE supports the functionality of the biometric system (e.g.: integration with the building's physical structure and door locks, audit functionality).
- It is assumed that all environmental factors are appropriate with respect to the used fingerprint sensor.
- The TOE environment provides a database for the biometric reference of enrolled users, whereby integrity and authenticity are ensured.
- The environment ensures a secure communication of security relevant data from and to the TOE.

- It is assumed that the environment provides a functionality to review the audit information of the TOE and to ensure that only authorised administrators have access to the audit logs.
- It is assumed that the TOE environment is free of viruses, trojans, and malicious software.

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 preparative user guidance (Ref 21a)).

17 The TOE is delivered as an application by the developer and developer will make changes to configuration based on preparative user guidance (Ref 21a)). as following:

a) Installation procedure.

b) Initial Setup (Data/Date Adjustment, Enrolment Form, User Enrolment, Multiple ID Enrolment, Auto ID Enrolment, Fingerprint verification).

c) Deleting user.

d) eJari NM 4000 Setting (Time Zone, Day Zone, Password, Communication, Door, Mode Menu and language).

1.8 Delivery Procedures

18 E-Jari v 4.0 is delivered to the user by the developer's authorised personnel.

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 E-Jari v 4.0 is used in accordance with guidance documentation.

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

a) E-Jari NM 4000 Operational Manual, Version 1.7, 29 November 2010.

2 Evaluation

22 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

23 The evaluation activities involved a structured evaluation of E-Jari v 4.0, including the following components:

2.1.1 Life-cycle support

24 An analysis of the E-Jari v 4.0 configuration management systems 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

25 The evaluators analysed the E-Jari v 4.0 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

26 The evaluators examined the E-Jari v 4.0 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

27 Testing at EAL1 consists of performing independent function test, and performing penetration tests. The E-Jari v 4.0 testing was conducted at CyberSecurity Malaysia MySEF where it was subjected to an independent functional and penetration tests. 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

28 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.

29 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Four independent functional tests were developed and performed by the evaluators to verify the TOE functionality as follows:

Table 2: Independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	TEST RESULT
This test group comprises a series of test cases to ensure security functions of TOE for audit records generation for relevant authentication and management events.	Security Audit	Display	PASS
This test group comprises a series of test cases on TOE security functions to ensure that there is no residual information exists in the TOE.	Residual Information Protection	No exact TSFI due to the SFR behaviour itself (FDP_RIP.2). Testing is done by showing the absence of any previous information on biometric parameters of the offered fingerprint.	PASS
This test group comprises a series of test cases on TOE security functions for identification and authentication of administrator (pin pad entry) and user (smartcard and fingerprint verification) using 1:1 matching.	Identification and Authentication	Display Contactless smartcard reader Fingerprint Sensor PIN pad	PASS
This test group comprises a series of test cases on TOE security functions for administrator's management function.	Security Management	Administrator Functions PIN pad Fingerprint Sensor Failure Message	PASS

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

2.1.4.2 Penetration Testing

31 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.

32 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential. The following factors have been taken into consideration during the penetration tests:

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

b) Specialist technical expertise required (specialist expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

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

33 The penetration tests focused on:

a) Compromise legitimate user privilege by hacking the TOE

b) User impersonation.

c) Denial of Service.

34 The results of the penetration testing note that there is no vulnerability 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

35 Tests conducted for the E-Jari v 4.0 produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

3 Results of the Evaluation

36 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 E-Jari v 4.0 performed by the CyberSecurity Malaysia MySEF.

37 The CyberSecurity Malaysia MySEF found that E-Jari v 4.0 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.

38 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 remain 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

39 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.

40 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.

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

3.2 Recommendation

42 In addition to ensure secure usage of the product, below are additional recommendations for E-Jari v 4.0 consumers:

a) Use the product only in its evaluated configuration;

b) The TOE should be installed in a physically secure environment to protect it against unauthorised access and destruction to its electronic environment;

c) To implement the TOE in its optional network features, it is advisable that the administrator installs and deploys the TOE in the network separated from the organisation internal and external network for efficient data communication to the external database use to store the users enrolled ID.

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] Security Target for E-Jari version 4.0, Version 0.24, 3 December 2010

[7] Evaluation Technical Report E-Jari v 4.0, Version 1.1, 3 December 2010

[8] E-Jari NM 4000 Operational Manual, Version 1.7, 29 November 2010

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
ST	Security Target
TOE	Target of Evaluation

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.
Minutiae	Minutiae is a term used to describe the points ("plot points") at which the ridges seen on a finger scan branch or end
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

Term	Definition and Source
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---