C020 Certification Report

Palm n' Go - Ezio Version 1.0

File name: ISCB-5-RPT-C020-CR-v1a
Version: v1a
Date of document: 21 July 2011
Document classification: PUBLIC

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

C020 Certification Report

Palm n' Go - Ezio Version 1.0

21 July 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:	C020 Certification Report - Palm n' Go - Ezio Version 1.0
DOCUMENT REFERENCE:	ISCB-5-RPT-C020-CR-v1a
ISSUE:	v1a
DATE:	21 July 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) 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 21 July 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	4 July 2011	All	Final Released.
v1a	21 July 2011	Page iv	Add the date of the certificate.

Executive Summary

Palm n' Go - Ezio Version 1.0 (hereafter referred as Palm n' Go) from Multimedia University is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 1 evaluation.

The TOE is a touch-less hand geometry and palm print authentication application. It provides the ability to verify a claimed identity of a human being using the subject's *palm vein pattern* as a unique characteristic of their body thus providing a method for controlling access.

The TOE works in verification mode only and does not provide biometric identification. Using Palm n' Go in an identification mode is considered outside the evaluated configuration. In this evaluation, it is assume that all authorised users have been successfully enrolled because the enrolment process is out of the evaluation scope.

The TOE also utilises a non-biometric mechanism (username and password) to identify and authenticate an administrator of the TOE to enforce an access control policy for controlling access and to the management functions of the TOE.

The TOE also provides the capability to capture audit records for events of interest associated with both the biometric identification and TOE configuration functions.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for Palm n' Go, 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 Palm n' Go 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 stratsec Security Evaluation Facility (STRATSEF) and completed on 6 June 2011.

The Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the Palm n' Go evaluation meets all the conditions of the MyCC Scheme requirements and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc.

It is the responsibility of the user to ensure that the Palm n' Go meets their requirements. It is recommended that a potential user of the Palm n' Go 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), Palm n' Go - Ezio Version 1.0 (hereafter referred as Palm n' Go), is a touch-less hand geometry and palm print authentication application developed using MMU's software development kit (SDK) called EzioSDK. It provides the ability to verify a claimed identity of a human being using the subject's *palm vein pattern* as a unique characteristic of their body thus providing a method for controlling access.

2 The TOE works in verification mode only and does not provide biometric identification. Using Palm n' Go in an identification mode is considered outside the evaluated configuration. In this evaluation, it is assume that all authorised users have been successfully enrolled because the enrolment process is out of the evaluation scope.

3 The TOE also utilises a non-biometric mechanism (username and password) to identify and authenticate an administrator of the TOE to enforce an access control policy for controlling access and to the management functions of the TOE.

4 The TOE also provides the capability to capture audit records for events of interest associated with both the biometric identification and TOE configuration functions.

1.2 TOE Identification

5 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	C020
TOE Name	Palm n' Go - Ezio Version 1.0
TOE Version	1.0
Security Target Title	Multimedia University Palm n' Go - Ezio Security Target
Security Target Version	1.3
Security Target Date	16 May 2011
Assurance Level	EAL 1
Criteria	Common Criteria Part 1, Common Criteria Part 2, Common Criteria Part 3.1 Revision 3 (Ref [2])
Methodology	Common Methodology for IT 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	Multimedia University, Faculty of Information Science & Technology (FIST) Multimedia University, Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia.
Evaluation Facility	STRATSEC.NET SDN BHD known as STRATSEF

1.3 Security Policy

6 The security policy of Palm n' Go is expressed by the set of security functional requirements which includes identification and authentication, auditing, and security management. Further details on these security policies may be found in Section 4.3 of the ST (Ref [6]).

1.4 TOE Architecture

7 Palm n' Go includes both logical and physical boundaries.

1.4.1 Logical Boundaries

8 The logical boundary consists of the security functionality of TOE is summarised below:

a) **Identification and Authentication** - The TOE requires the user to identify and authenticate themselves before accessing any information and performing any actions. The TOE can verify the claimed identity of a user by using their *palm vein pattern as* a unique characteristic of their body. For the TOE administrator identification and authentication will be using a non-biometric mechanism (ID and password) provided by the TOE.

b) **Auditing -** The TOE captures success/failures of user and administrator verification. Audit data can be reviewed by the administrator.

c) **Security Management -** The TOE provides various security management functions such as user management, sensitivity of the capture device, etc to ensure efficiency and secure management of the TOE. Only administrator is allowed to have access to the security management functions.

1.4.2 Physical Boundaries

9 The TOE is an application installed on a Windows-based operating system with Microsoft .NET framework version 4.0 and underlying suitable hardware. The underlying operating system provides reliable timestamps to the TOE.

10 Administrator can access the audit records and also the TOE configuration using the management portal which provides a policy management environment for the TOE.

11 Figure 1 below identifies the various components of the Palm n' Go and the scope of the evaluation.

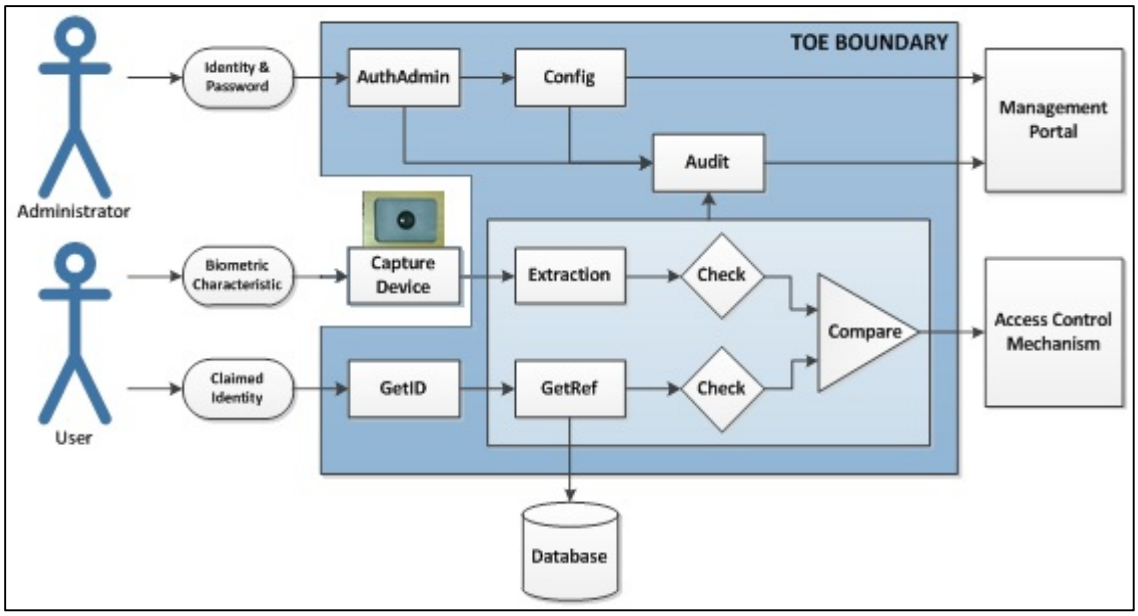

Figure 1: Components of Palm n' Go

12 The following Table 2 describes the components of Palm n' Go which includes in the TOE boundary.

Table 2: Components of Palm n' Go

Components	Description
AuthAdmin	This component is responsible for identification and authentication of the administrator with other means than the biometric verification mechanism. This mechanism is a classical identification and authentication component that is realised through a password based mechanism. Authentication of the TOE administrator needs to be successful before he is allowed to configure security relevant settings of the TOE.
Configure	This component provides an interface for the administrator to set security relevant TOE parameters. This component is especially used to configure the threshold setting for the comparator component and to determine audit events.
Audit	This component of the TOE records security relevant events to ensure that information exists to support effective security management.
GetID	This component is responsible for getting the user's claimed identity. The system uses the claimed ID to determine, which biometric reference has to be used for comparison. Furthermore, this component provides a mandatory user visible interface.

Components	Description
Capture Device	An infrared vein scanner/camera that supports Microsoft DirectX SDK and able to provide a digital representation of a hand vein image.
GetRef	This component is responsible for getting the stored (already enrolled) biometric reference related to a claimed user's identity.
Check	This component ensures the minimum quality requirements regarding the biometric references. It can be differentiated into integrity and authenticity check during the process of getting the biometric reference as well as the quality check of the biometric information during the processing of the live biometric characteristics.
Compare	This important component compares the enrolled biometric reference with the Biometric Live Record (BLR) and includes the determination whether these records match or not. It produces a value that shows how well the biometric reference and BLR match. To get a successful/failed return value from the biometric system, the comparator considers a threshold during the matching process. If the biometric reference and the BLR are more similar than demanded by the threshold, the return value is success, otherwise it is fail. An "Exact match" comparison will result in a positive verification and is recorded in the audit log.

1.5 Clarification of Scope

13 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) **Auditing** – provides the capability to generate the audit trail for:

i) Start-up and shutdown of the audit functions

ii) Success or failure of user authentication

iii) Success or failure of administrator authentication

iv) Changing the sensitivity settings of the capture device

v) Changing the threshold of the comparator

vi) Changing the number of pictures of the palm vein the capture device take

vii) Enrolment of users

viii) Creation and deletion of users

ix) Turning and switching off audit mechanism, clearing audit records

All the events are recorded with the time (provided by the underlying operating system), user's ID, type of event. Audit records will be stored in the database.

b) **Identification and Authentication –** provides a platform to identify and authenticate user.

The user will enter their user ID and have their palm vein patterns captured by the capture device. The TOE gets the user ID and references it to the database to get the enrolled biometric reference and compares it to the BLR (the TOE will use the captured vein pattern and convert them to a binary string format). The result of the comparison (authentication successful or not) is returned to the application, which can then decide to allow further actions to the user.

The TOE also provides another verification mechanism to the TOE administrator. Administrator will first identify himself by entering a user ID. This can be done by a keypad system or touch screen user interface that will be handled by the application developer using the TOE. The TOE will use the user ID and check the database to get the password reference of the administrator.

The administrator will enter his password and the TOE compares the password with the password reference retrieved from the database using the user ID as reference previously. The TOE will allow the access to the management functions of the TOE only after a successful verification of the TOE administrator.

c) **Security Management** – provides platform for the TOE administrator to have access to the following security management functions:

i) **Changing the sensitivity settings of the capture device**: this setting deals with the quality of the picture taken by the infra-red camera of the vein patterns. The default value for this is 5.

ii) **Changing the threshold of the comparator**: this setting deals with the threshold of the comparator. A high threshold level will result in a lower False Acceptance Rate and higher False Rejection Rate and vice versa. Administrator will need to configure this according to the requirements of the organization that uses the TOE and the application. The default value for this is 5.

iii) **Changing the number of pictures of the palm vein the capture device takes**: this setting deal with the number of pictures the extraction engine of the TOE takes to form the binary string for the biometric reference. More pictures will result in a better quality biometric reference and vice versa. The default value for this is 3.

iv) **Enrolment of users**: enrolment of user can only be carried out in front of the administrator. The user will enter his biometric reference to the system and it will be stored into the database.

v) **Creation and deletion of users**: administrator can create new user ID as well as deletion of users from the system.

vi) **Turning and switching off audit mechanism**: The audit mechanism can be turned off and on by the administrator.

14 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.

15 Functions and services which are not included as part of the evaluated configuration are as follows:

a) The physical or logical point beyond which information or assets are protected by a biometric system;

b) The TOE works in verification mode only and does not provide biometric identification. Using Palm n' Go in an identification mode is considered outside the evaluated configuration.

c) The enrolment process is also considered out the scope of the evaluation as the TOE assumes that all authorised users have been successfully enrolled.

d) A Hardware server;

e) Capture device (infrared vein scanner/camera);

f) Windows-based operating system (Windows XP/Vista/ 7);

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

h) Other supporting software:

i) Microsoft Visual Studio 2010 (or Version 10)

ii) Microsoft .NET framework version 4.0.

1.6 Assumptions

16 This evaluation was performed at EAL1. Therefore, no assumptions for the TOE were defined in the ST (Ref [6]).

1.7 Evaluated Configuration

17 The evaluated configuration of the TOE covers verification mode only. Other than this configuration is considered outside the evaluated configuration.

18 The TOE is to be configured using the minimum hardware and software requirements as specified in the guidance documentation (Ref [8]) and as specified in the ST (Ref [6]).

19 The TOE is available on a CD and is delivered by a trusted entity to the end users. TOE administrator will be responsible for the installation and configuration of the TOE based on the guidance documentation (Ref [8]).

1.8 Delivery Procedures

20 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.

21 Based on the guidance documentation (Ref [8]), the TOE shall be delivered on a CD by the trusted entity to the end user. The TOE administrator is responsible to check the integrity of the content, installed, configured, and set up in accordance with the guidance documentation (Ref [8]).

1.9 Documentation

22 To ensure the secure usage of the product, it is important that the Palm n' Go is used in accordance with guidance documentation.

23 The following documentation is used by the developer as guidance to use the EzioSDK to build custom applications:

a) Palm n' Go – Ezio SDK Developer Guide, Developer Guide.chm.

b) Palm n' Go – Ezio SDK Functional Specification, version 1.0.0.0, 20 August 2010.

24 The following documentation is provided to the end user as guidance to ensure secure installation and operation of the product:

a) Multimedia University Palm n' Go – Ezio Guidance Documentation (Ref [8]).

b) Palm n' Go – Ezio SDK Demo Application Guide, version 1.0, 29 October 2010.

2 Evaluation

25 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

26 The evaluation activities involved a structured evaluation of Palm n' Go, including the following components:

2.1.1 Life-cycle support

27 An analysis of the Palm n' Go Version 1.0 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

28 The evaluators analysed the Palm n' Go 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

29 The evaluators examined the Palm n' Go 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

30 Testing at EAL1 consists of performing independent function test, and performing penetration tests. The Palm n' Go testing was conducted by tester from stratsec at Multimedia University Lab 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

31 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.

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

Table 3: Independent Functional Testing

Description	Security Function	TSFI	Results
To test that TOE is able to generate an audit record of the auditable events.	Auditing	User Interface	**PASS.** Result as expected.
To test that TOE is able to associate each auditable event with identity of the user caused the event.	Auditing	User Interface	**PASS.** Result as expected.
To test that TOE is able to maintain the following list of security attributes belonging to individual users	Identification and Authentication	User Interface Database Interface	**PASS.** Result as expected.
To test that user must successfully authenticate before any action can be done.	Identification and Authentication	User Interface Database Interface Device Interface	**PASS.** Result as expected.
To test that TOE requires multiple authentication such as biometric and non- Biometric verification mechanism.	Identification and Authentication	User Interface Database Interface	**PASS.** Result as expected.
To test that a message indicating verification efforts are in progress is shown to user while biometric authentication is in progress.	Identification and Authentication	User Interface Database Interface Device Interface	**PASS.** Result as expected.
To test that TOE require each user to be successfully identified before allowing any action on	Identification and Authentication	User Interface Database	**PASS.** Result as expected.

behalf of that user.		Interface	
To test that TOE shall restrict audit function such as enable, disable or modify to administrator.	Security management	User Interface	**PASS.** Result as expected.
To test that TOE shall restrict the ability to change_default, query, modify, delete, clear the following configuration to administrator	Security management	User Interface	**PASS.** Result as expected.
To test that only secure values are accepted. The secure values are biometric reference records, sensitivity of the capture device, number of pictures of veins taken by the capture device and threshold of the comparator.	Security management	User Interface	**PASS.** Result as expected.
To test that the roles of users and TOE administrator are maintain and able to associate users with roles.	Security management	User Interface	**PASS.** Result as expected.
To test that TOE shall be capable of performing the security management functions specified in the ST.	Security management	User Interface	**PASS.** Result as expected.

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

2.1.4.2 Penetration Testing

34 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.

35 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.

36 The penetration tests focused on :

a) Exploit .Net;

b) Password brute force.

c) Impersonation as real user (fake palm).

37 The results of the penetration testing note that there is no exploitable 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

38 Tests conducted for the Palm n' Go produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

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

3 Result of the Evaluation

40 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 Palm n' Go performed by the STRATSEC Security Evaluation Facility (SEF) which known as STRATSEF.

41 The STRATSEF found that Palm n' Go 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.

42 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

43 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.

44 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.

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

3.2 Recommendation

46 In addition to ensure secure usage of the product, below are additional recommendations for Palm n' Go Version 1.0 consumers:

a) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

b) The TOE should be implemented as part of a broader biometric system that effectively controls the enrolment and user management components of a biometric capability.

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

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] Multimedia University Palm n' Go - Ezio Security Target, Version 1.3, 16 May 2011.

[7] Evaluation Technical Report EAL1 Evaluation of Palm N' Go - Ezio, Version 1.2, 6 June 2011.

[8] Multimedia University Palm n' Go – Ezio Guidance Documentation, v1.2, 28 March 2011

A.2 Terminology

A.2.1 Acronyms

Table 4: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Standards Organisation
ISCB	Information Security Certification Body
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 5: Glossary of Terms

Term	Definition and Source
Biometric	A measurable physical characteristic or personal behavioural trait used to recognise the identity of a user or verify a claimed identity.
Biometric Live Record (BLR)	Includes the actual biometric data (actual biometric characteristic and user identity) to be verified against the biometric reference record.
Biometric Reference Record (BRR)	An object containing a Biometric Reference
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
Comparison	The process of comparing biometric data with a previously stored biometric reference
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.
False Rejection Rate (FRR)	Proportion of verification transactions with truthful claims of identity that are incorrectly denied
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.

Term	Definition and Source
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.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Portal	The physical or logical point beyond which information or assets are protected by a biometric system.
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.
Threshold	A parametric value used to convert a matching score to a decision.

--- END OF DOCUMENT ---