C049 Certification Report

PKID ECC Generator v1.1

File name: ISCB-5-RPT-C049-CR-v1a
Version: v1a
Date of document: 20 November 2013
Document classification: PUBLIC

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

C049 Certification Report

PKID ECC Generator v1.1

20 November 2013

ISCB Department

CyberSecurity Malaysia

Level 5, Sapura@Mines,

No 7 Jalan Tasik, The Mines Resort City

43300 Seri Kembangan, Selangor, Malaysia

Tel: +603 8992 6888 □ Fax: +603 8992 6841

http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C049 Certification Report – PKID ECC Generator v1.1
DOCUMENT REFERENCE:	ISCB-5-RPT-C049-CR-v1a
ISSUE:	v1a
DATE:	20 November 2013

DISTRIBUTION:	UNCONTROLLED COPY – FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 5, Sapura@Mines

No 7, Jalan Tasik,

The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

Printed in Malaysia

Foreword

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 20 November 2013, 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 4 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 4 (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	6 November 2013	All	Final Released.
v1a	20 November 2013	Page iv	Add the date of the certificate.
		Paragraph 30	Rewording the paragraph to summarise the requirement of Life-cycle support (ALC) for EAL2.

Executive Summary

PKID ECC Generator v1.1 from WannaStation.com Sdn Bhd is the Target of Evaluation (TOE) for the Evaluation Assurance Level 2 (EAL2) evaluation.

PKID ECC Generator v1.1 is software that generates public and private keys based on a user definable and recognisable ID of ASCII characters or known as PKID. Therefore, the public and private keys have distinctive and unique attributes of each user. A user may choose a PKID unique to himself or herself, such as PC/Notebook MAC address, IMEI number and email address. A chosen PKID will become the seed to generate a public and private key through a series of key generation processes. The generated public and private keys are tied to the chosen PKID. Using algorithm based on elliptic curve encryption algorithm, much smaller key size will be used and desirable as it allows the application on PC, smart phones or mobile communication devices for multi-function security applications.

The evaluation scope only covers:

a) the generation of the Master Key based on random keystroke input from client organisation. The Master Key will be used to generate the customised PKID ECC Generator specific to that client organisation, and

b) the generation of public and private keys together with the access code, based on the user's PKID entered manually to the generated customised PKID ECC Generator.

Hardware, software like automation Detection Software and operating system, and revocation, destruction and recovery of keys are not covered in the TOE scope.

The scope of evaluation covers major security features as follows:

a) Authentication – in order to generate the customised PKID ECC Generator which is specific to the client organisation, authentication is required by the TOE administrator before the Master Key can be imported into the generator. Authentication is also required by the TOE administrator to access the customised PKID ECC Generator before any further action is permitted.

b) Security Management – provides management of TOE security functions during customisation of the PKID ECC generator such as setting the access code for the generated Master Key, management of public and private keys, and management of administrator credential in the customised PKID ECC generator.

c) Cryptographic Support – provides generation of Master Key during customisation of the PKID ECC Generator based on the random keystroke input from client

organisation, and generation of public and private keys together with access code, in customised PKID ECC Generator using specified encryption algorithm.

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

Additional testing was conducted to validate the generation of the Master Key, and also the public and private keys. Based on the results, it can be summarised that the TOE generates non-repeatable Master Key during customisation of the PKID ECC Generator and the TOE is using Elliptic Curve Cryptography (plane curve) in generating random public and private keys.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2). This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]). The evaluation was performed by MySEF CyberSecurity Malaysia evaluation facility and completed on 7 October 2013.

The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in 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 user to ensure that PKID ECC Generator meet their requirements. It is recommended that a potential user of PKID ECC Generator 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), PKID ECC Generator v1.1 (hereafter referred as PKID ECC Generator) is a software that is used to generate public and private keys based on a user definable and recognisable ID of ASCII characters or known as PKID.

2 A user may choose a unique PKID to himself or herself such as from PC/Notebook MAC address, IMEI number, or email address. A chosen PKID will become the seed to generate a public and private key through a series of key generation processes.

3 The TOE uses cryptographic algorithm based on elliptic curve encryption algorithm to generate the public and private keys that are tied to the chosen PKID. Using algorithm based on elliptic curve encryption algorithm, much smaller key size will be used and desirable as it allows the applications on PC, smart phones or mobile communication devices for multi-function security applications. Depending on the PKID, the public and private keys generated by the TOE can be used on various platform as follows:

Table 1: Input and Output Platform

PKID	Output Platform
PC/Notebook MAC address	PC/Notebook (for audio file encryption/ decryption)
IMEI number	Mobile phone (for file encryption/ decryption, not for SMS)
Email address	PC/Notebook (for file encryption/ decryption)

4 The evaluation scope only covers:

a) the generation of the Master Key based on random keystroke input from client organisation. The Master Key will be used to generate the customised PKID ECC Generator specific to that client organisation, and

b) the generation of public and private keys together with the access code, based on the user's PKID entered manually to the generated customised PKID ECC Generator.

5 Hardware, software like automation Detection Software and operating system, and revocation, destruction and recovery of keys are not covered in the TOE scope.

6 In the context of the evaluation, the TOE is expected to provide the following major security feature:

a) **Authentication** – in order to generate the customised PKID ECC Generator which is specific to the client organisation, authentication is required by the

TOE administrator before the Master Key can be imported into the generator. Authentication is also required by the TOE administrator to access the customised PKID ECC Generator before any further action is permitted.

b) **Security Management** – the TOE allows the administrator to manage the TOE security functions in the customised PKID ECC Generator. This includes the management of administrator password, generation of public and private keys, and exporting the keys upon request. The TOE is also capable to set the access code for the generated Master Key during the customisation of the PKID ECC Generator.

c) **Cryptographic Support** – the TOE provides generation of Master Key during customisation of the PKID ECC Generator based on the random keystroke input from client organisation, and generation of public and private keys together with access code, in customised PKID ECC Generator using specified encryption algorithm.

1.2 TOE Identification

7 The details of the TOE are identified in Table 2 below.

Table 2: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C049
TOE Name	PKID ECC Generator
TOE Version	v1.1
Security Target Title	PKID ECC Generator v1.1 Security Target
Security Target Version	v1.0
Security Target Date	7 October 2013
Assurance Level	Evaluation Assurance Level 2 (EAL2)
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4 (Ref [2])
Methodology	Common Evaluation Methodology for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL2

Sponsor and Developer	WannaStation.com (M) Sdn Bhd Lot 1109-A, 10th Floor Kelana Parkview Tower, No.1, Jalan SS6/2, Kelana Jaya 47301 Petaling Jaya, Selangor Malaysia
Evaluation Facility	CyberSecurity Malaysia MySEF

1.3 Security Policy

8 The TOE user is the administrator who is responsible to manage the TOE security features (Ref 6). In order to ensure the security of the TOE, only authorised administrators are assigned by the organisation to have access to the TOE. Authorised administrators shall be authenticated before allowing any other actions (refer to Section 4.3 and Section 7.2 of the ST (Ref [6])).

1.4 TOE Architecture

9 The TOE includes both logical and physical boundaries which are described in Section 2.3 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

10 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) **Authentication**

Administrators are required to insert access code for authentication before importing the generated Master Key into the generator. Once authenticated, the Master Key will be used to generate the customised PKID ECC Generator for that specific client organisation.

Authentication is also required by the TOE administrator to access the customised PKID ECC Generator before the TOE allows any other actions. The TOE also provides a mechanism to verify the new password entered is minimum 8 characters.

b) **Security Management**

The security management of the TOE occurs during:

i) customisation of the PKID ECC Generator – after the Master Key had been generated using specified cryptographic key generation, an access code is set by the TOE administrator for the generated Master Key, and

ii) customised PKID ECC Generator – authenticated TOE administrator are capable to perform the following functions:

(a) Change administrator password – in order to change the password, the administrator needs to enter current and new password. The

current password entered will be checked against the profile in the TOE. If it matches, then the new password entered will be checked to meet requirement of minimum 8 characters.

(b) Generate public and private keys – the administrator generates the public and private keys together with access code for the users, based on the PKID supplied by the users.

(c) Export keys – the public and private keys can be exported by the administrator upon user's request such as the case where the user lost the keys. Generated public and private keys are stored in designated folder in the TOE. Keys that are going to be exported will be stored in separate designated folder where the keys are ready for copying and distribution to the users.

c) **Cryptography Support**

The TOE provides generation of Master Key for specific client organisation based on the random keystroke input from the client organisation. The unique Master Key will be used to generate the customised PKID ECC Generator. This is important to ensure that no one can duplicate the Master Key without having the same input from the client organisation. Master Key shall be generated using specified cryptography key generation which is non-repeatable with 320 bit key size.

Once the Master Key had been generated, it will be imported into the generator in order to generate the customised PKID ECC Generator. Then the authorised TOE administrator will access the customised PKID ECC Generator to generate public and private keys, together with access code, by using standard Elliptical Curve Cryptographic (plane curve) with 320 bit key size. To import the Master Key, access code is required for authentication.

The generated public and private keys are unique for each user's PKID. For example, files encrypted using the public key generated for a MAC address can only be decrypted using the corresponding private key on the PC/Notebook with the same MAC address. The new generated keys will be stored in the designated folders before it can be exported to the user or other storage medium for backup.

1.4.2 Physical Boundaries

11 The TOE is software used for the generation of public and private keys that are generated based on a user definable and recognisable ID of ASCII characters or known as PKID.

12 The TOE executes on a computer running Windows 2003 Server, with required non-TOE hardware, and software specified in Section 2.2.3 of the Security Target (Ref [6]). The non-TOE hardware and software are not in the scope of this evaluation.

13 Figure 1 below shows the components of PKID ECC Generator v1.1 which consists of the TOE components.

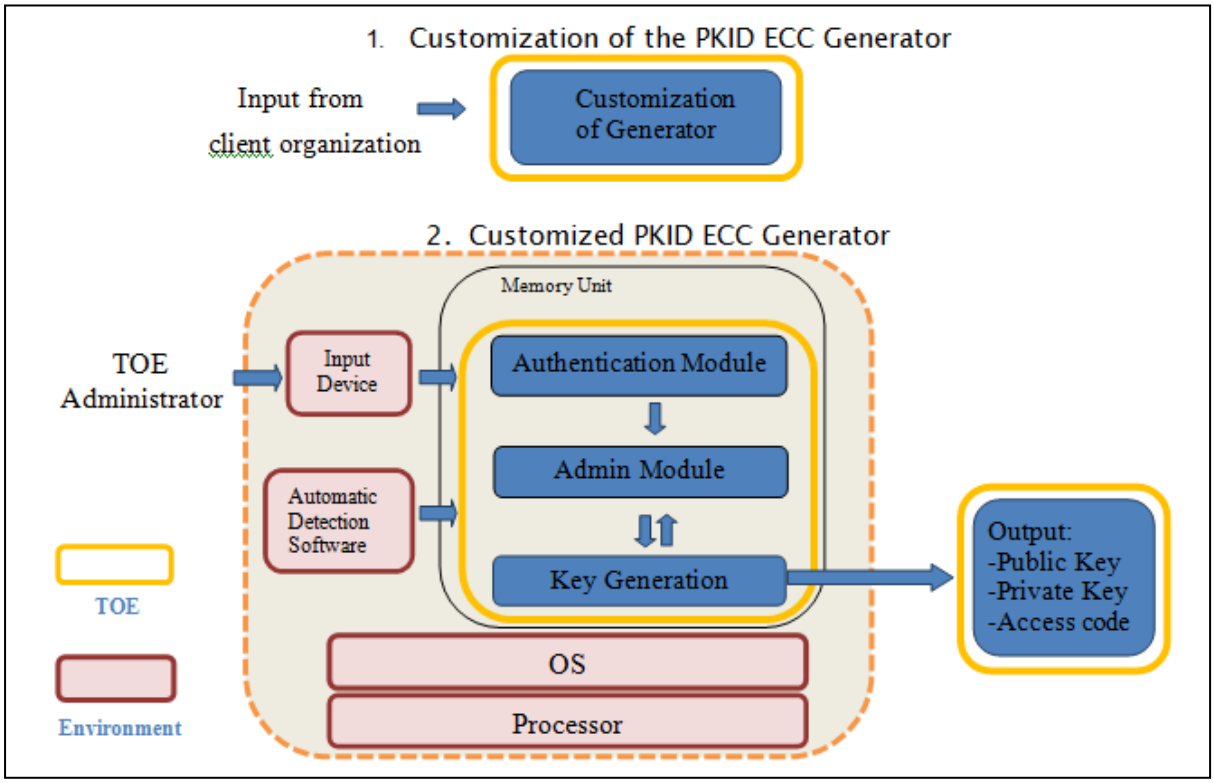

Figure 1: TOE Physical Scope

14 The scope of the evaluation only covers 2 components of the PKID ECC Generator v1.1 as follows:

a) Customisation of the PKID ECC Generator

This component provides customisation of client organisation's random keystroke input in order to generate Master Key and customised PKID ECC Generator.

The Master Key is unique for each client organisation. This is important to ensure that no one can duplicate the Master Key without having the same input from the client organisation. An access code is set by the TOE administrator for the generated Master Key. TOE administrator is required to insert the access code for authentication before importing the generated Master Key into the generator. Once authenticated, the Master Key will be used to generate the customised PKID ECC Generator for that specific client organisation.

b) Customised PKID ECC Generator

Customised PKID ECC Generator is unique for each client organisation. It is used by the authorised TOE administrator to generate public and private keys together with access code, based on the PKID (seed) supplied by the user either

manually keyed in or automatic detected. In this evaluation, only manual PKID key in was covered and the TOE resides in a standalone server which is not connected to any network.

Other than that, within the scope of the evaluation, customised PKID ECC Generator is used to manage the TOE which includes:

i) Change administrator password – in order to change the password, the administrator needs to enter the current and new password. The current password entered will be checked against the profile in the TOE. If it matches, then the new password entered will be checked to meet requirement of minimum 8 characters.

ii) Export keys – the public and private keys can be exported by the administrator upon user's request such as the case where the user lost the keys. Generated public and private keys are stored in designated folder in the TOE. Keys that are going to be exported will be stored in separate designated folder where the keys are ready for copying and distribution to the users.

1.5 Clarification of Scope

15 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 secure communication in accordance with user guidance that is supplied with the product.

16 Section 1.4 of this document described the scope of the evaluation which was limited to those claims made in the Security Target (Ref [6]).

17 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.

1.6 Assumptions

18 This section summarises the security aspects of the environment/configuration in which IT product is intended to operate. Consumers should understand their own IT environments and requirements for the secure operation of the TOE as defined in subsequent sections and in the Security Target (Ref [6]).

1.6.1 Usage assumptions

19 Assumptions for the TOE usage as listed in Security Target are:

a) The authorised TOE Administrator is non-hostile, keeps the Master Key CD in a secure place and follows guidance documentation accordingly.

1.6.2 Environment assumptions

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

a) The TOE and its environment are physically secure and managed by authorised TOE Administrator.

b) PKID received from user as the seeds for the generation of public and private key is in good condition without being tampered.

c) The TOE environment will destroy cryptographic keys generated by the TOE.

d) Client applications will handle correct operation of encryption and decryption using key generated by TOE.

e) The TOE environment will handle revocation of the cryptographic keys.

f) The Operating System where the TOE executed and all third party applications installed are trusted and do not perform malicious actions to compromise the operation of the TOE. The TOE resides in a standalone server without connection to any network.

1.7 Evaluated Configuration

21 The TOE is software used for the generation of public and private keys that is generated based on a user definable and recognisable ID of ASCII characters or known as PKID.

22 The TOE executes on a computer running Windows 2003 Server, with required non-TOE hardware, and software specified in Section 2.2.3 of the Security Target (Ref [6]).

23 The assurance gained via evaluation applies specifically to the TOE in the defined evaluated configuration according to the documented preparative user guidance (Ref 27b)).

1.8 Delivery Procedures

24 PKID ECC Generator is delivered to the customers using delivery procedure (Ref 27a)) which ensures that the PKID ECC Generator is securely transferred from development environment into the responsibility of the user, and protected against tampering and impersonation.

25 Typically, PKID ECC Generator and printed based manual is hand delivered by WannaStation.com (M) Sdn Bhd authorised personnel. Then it will be installed by WannaStation.com (M) Sdn Bhd authorised personnel together with the customer to ensure the correct and legitimate version is delivered. After successfully installed, they will proceed with customisation of the product for the customer.

1.9 Documentation

26 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage of the product.

27 The following documentation is provided by the developer to the end user as guidance to ensure secure delivery, installation, and operation of the product:

a) PKID ECC Generator v1.1 ALC (PKIDECCGEN-ALC-v1.0-071013), v1.0, 7 October 2013

b) PKID ECC Generator v1.1 Preparative Guidance (PKIDECCGEN-AGDPRE-v1.3-071013), v1.3, 7 October 2013

c) PKID ECC Generator v1.1 Administrator Guidance (PKIDECCGEN-AGD_OPE-v1.3-230913), v1.3, 23 September 2013.

2 Evaluation

28 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 4 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 4 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2 (EAL2). 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

29 The evaluation activities involved a structured evaluation of the TOE, including the following components:

2.1.1 Life-cycle support

30 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

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

2.1.2 Development

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

33 The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that, it provides a complete, accurate, and high-level description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

34 The evaluators examined the TOE security architecture description; they determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

2.1.3 Guidance documents

35 The evaluators examined the TOE 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

36 Testing at EAL2 consists of assessing developer tests, perform independent function test, and perform penetration tests. The TOE testing was conducted by evaluators from CyberSecurity Malaysia MySEF at CyberSecurity Malaysia MySEF lab. 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 Assessment of Developer Tests

37 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator).

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

2.1.4.2 Independent Functional Testing

39 At EAL2, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing sample of the developer's test plan, and creating test cases that augmented developer tests.

40 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 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
Test Group comprises a series of test cases on TOE security functions of Authentication.	Authentication	Customisation of Generator TSFI	**PASS**. Result as expected
Test Group comprises a series of test cases on TOE security functions of	Security Management	• Login TSFI • Admin TSFI	**PASS**. Result as expected

Security Management			
Test Group comprises a series of test cases on TOE security functions of Cryptographic support	Cryptographic Support	• Generate public and private key TSFI • Customisation of Generator TSFI	PASS. Result as expected

41 All testing performed by evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Penetration Testing

42 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, functional specification, TOE design, and security architecture description.

43 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant 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 (elapse time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE design and operation;

d) Window of opportunity; and

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

44 The penetration tests focused on:

a) Software Based Key-logger

b) RAM analysis using HEX editor

c) Reverse engineering

d) Duplicate PKID generator library file

e) SQL injection

f) Brute Force

g) File extension attack

h) Open PKID file

45 The results of the penetration testing note that there is no residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated

configuration and in a secure environment as specified in Section 2.2.3 of the Security Target (Ref [6]).

2.1.4.4 Testing Results

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

47 Additional testing was conducted to validate the generation of the Master Key, and also the public and private keys. Based on the results, it can be summarised that the TOE generates non-repeatable Master Key during customisation of the PKID ECC Generator and the TOE is using Elliptic Curve Cryptography (plane curve) in generating random public and private keys.

48 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

49 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 PKID ECC Generator v1.1 performed by CyberSecurity Malaysia MySEF.

50 CyberSecurity Malaysia MySEF found that PKID ECC Generator v1.1 upholds the claims made in the Security Target (Ref [6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) assurance level 2 (EAL2).

51 Certification is not 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. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

52 EAL2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

53 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

54 EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

55 In addition to ensure secure usage of the product, below are additional recommendations for PKID ECC Generator v1.1 users:

a) A strict adherence to guidance documentations and procedures provided by the developer are highly recommended.

b) User needs to ensure that the TOE and its environment are physically secure and managed by authorised TOE Administrator.

c) User needs to ensure that the operating system where the TOE executed and all third party applications installed are trusted and do not perform malicious actions to compromise the operation of TOE. The TOE resides in a standalone server which is not connected to any network.

d) Potential users of the TOE are advised that some functions and services, such as:

i) revocation, destruction and recovery of the public and private keys,

ii) underlying hardware, and

iii) software such as automation Detection Software, operating system, client applications that use the keys generated by the TOE etc.

were not been evaluated. Potential consumers of the TOE should carefully consider their requirements for using those functions and services. Potential users should test these functions and services first before deployment by the TOE.

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 4, September 2012.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

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

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

[6] PKID ECC Generator v1.1 Security Target, v1.0, 7 October 2013.

[7] E032 Evaluation Technical Report for PKID ECC Generator v1.1, v1, 7 October 2013.

A.2 Terminology

A.2.1 Acronyms

Table 4: List of Acronyms

Acronym	Expanded Term
ASCII	American Standard Code for Information Interchange
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ID	Identity
IEC	International Electrotechnical Commission
IMEI	International Mobile Station Equipment Identity
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MAC address	Media access control address
MyCB	Malaysian Common Criteria Certification Body

Acronym	Expanded Term
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
PRNG	Pseudorandom Number Generator
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

A.2.2 Glossary of Terms

Table 5: 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
Client Organisation	Consumer of the product or the organisation that uses the certified product within their infrastructure.
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.

Term	Definition and Source
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.
PKID	Any definable and recognisable ID of ASCII characters such as PC/Notebook MAC address, IMEI number, or email address that will be used as the seed to generate a public and private keys.
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.
TOE Administrator	Any human users outside the TOE that manages and interacts with the TOE.
User	Any human users outside the TOE that provides the definable and recognisable ID of ASCII characters or known as PKID, such as PC/Notebook MAC address, IMEI number, or email address, for the generation of his/her public and private keys.

--- END OF DOCUMENT ---