MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity
MALAYSIA

C094 Certification Report

ePassport Application on MOS version 1.0.0

File name: ISCB-3-RPT-C094-CR-V1
Version: v1
Date of document: 8 April 2019
Document classification: PUBLIC

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

CyberSecurity Malaysia
(726630-U)

T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

Securing Our Cyberspace

C094 Certification Report

ePassport Application on MOS version 1.0.0

8 April 2019
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:	C094 Certification Report
DOCUMENT REFERENCE:	ISCB-3-RPT-C094-CR-V1
ISSUE:	v1
DATE:	8 April 2019

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 8 April 2019, 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).

Reproduction of this report is authorised provided the report is reproduced in its entirety.

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 using the Common Methodology for IT Security Evaluation, version 3.1 revision 5 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 (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
d1	3 April 2019	All	Initial draft
v1	5 April 2019	All	Changes after CSM MySEF and developer's revision

Executive Summary

The Target of Evaluation (TOE) is the ePassport Application on MOS version 1.0.0, which implemented as contact/contactless integrated circuit chip of an electronic travel document programmed according to ICAO Doc 9303 Machine Readable Travel Documents ([ICAO]) and additionally providing the Extended Access Control according to BSI TR-03110 ([TR-03110]). The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE) according to Protection Profile BSI-CC-PP-0068-V2 Machine Readable Travel Documents using Standard Inspection Procedure with PACE (PACE PP) ([PP-0068]).

The scope of the evaluation is defined by the Security Target (Ref [6]) which identifies assumptions made during the evaluation, the intended environment for the TOE, the security functional 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.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 4 (EAL4) augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5. 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 Cybersecurity Malaysia MySEF (Malaysia Security Evaluation Facility) collaborated with external SEF, JTSEC Beyond IT Security, Spain. The evaluation was completed on 21 March 2019.

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 http://www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at http://www.commoncriteriaportal.org

It is the responsibility of the user to ensure that ePassport Application on MOS version 1.0.0 meets their requirements. It is recommended that a potential user of the TOE 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 MCS Multi-Application Operating System (MOS) is a secure and powerful chip operating system purpose designed for trusted ID applications, especially e-passport and possibly ISO-compliant driving license and national ID. Its key features are:

a) File manager based on the ISO/IEC 7816 standard;

b) Global Platform Card Manager;

c) Early Lifecycle Manager; and

d) Biometric match-on-chip (optional).

2 The TOE resides on the hardware known as STMicroelectronics C01 platform featuring of cryptographic library NESLIB (optional feature) and derivative devices as provided details as below:

Table 1: IC Configuration values

Features	Possible values
I/O mode	Contact only, Dual Mode, Contactless only
NVM size	480 Kbytes
Nescrypt	Active
MIFARE support (Crypto1 + LPU)	Inactive
Capacitor	20pF, 68pF

3 The TOE hardware security target name is ST31G480 C01 includes features of cryptographic library Neslib (optional), and technologies MIFARE® DESFire® EV1(optional) and MIFARE Plus® X (optional) Security Target for Composition ([ST31G_ST]).

1.2 TOE Identification

4 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	C094
TOE Name	ePassport Application on MOS
TOE Version	1.0.0
Security Target Title	Security Target of ePassport Application on MOS
Security Target Version	1.0.0
Security Target Date	26 February 2019
Assurance Level	Evaluation Assurance Level 4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5
Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3])
Protection Profile Conformance	Protection Profile – Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE (EAC PP), version 1.3.2, BSI-CC-PP-0056-V2-2012-MA-02.
Common Criteria Conformance	CC Part 2 Extended CC Part 3 Conformant Package conformant to EAL 4 Augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5
Sponsor	MCS Microsytems Sdn Bhd
Developer	MCS Microsytems Sdn Bhd
Evaluation Facility	Cybersecurity Malaysia MySEF
Evaluation Facility of External Provider	JTSEC Beyond IT Security, Facilities located at CEG Building, Office 2B, Abeto Street, CP 18230, Atarfe, Granada, Spain

1.3 Security Policy

5 There are several organisational security policy that has been defined regarding the use of the TOE as below:

a) **P.Sensitive_Data.** Privacy of sensitive biometric reference data;

b) **P.Personalisation.** Personalisation of the travel document by issuing state or organisation only;

c) **P.Pre-Operational.** Pre-operational handling of the travel document;

d) **P.Card_PKI.** PKI for Passive Authentication (issuing branch);

e) **P.Trustworthy_PKI.** Trustworthiness of PKI;

f) **P.Manufact.** Manufacturing of the travel document's chip; and

g) **P.Terminal.** Abilities and trustworthiness of terminals.

6 Section 3.3 of the Security Target (Ref [6]) defines that the TOE shall comply with security rules, procedures, practice or guidelines imposed by an organisation upon its operations.

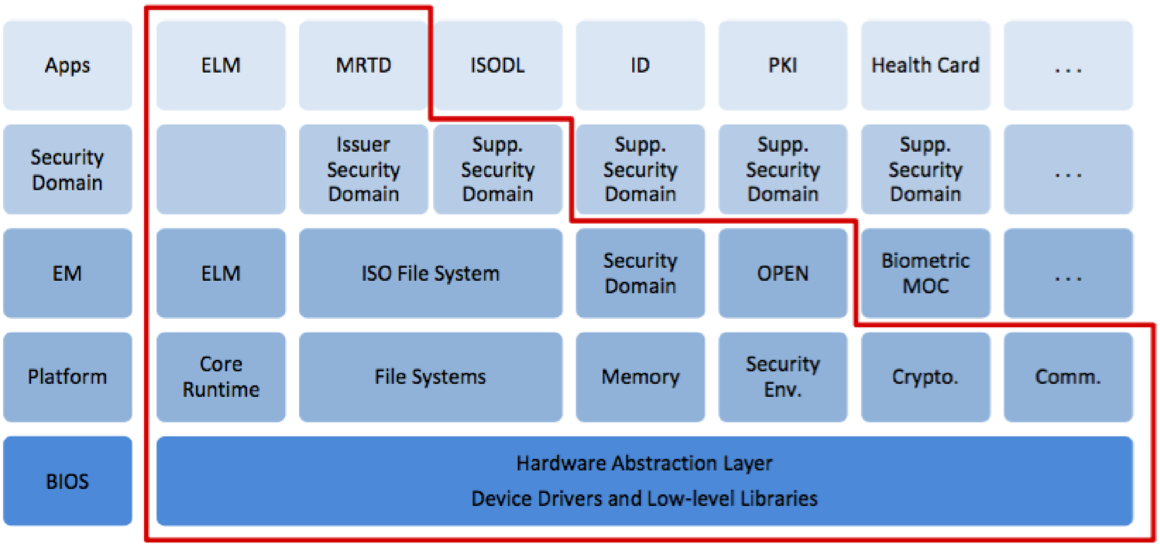
1.4 TOE Architecture

7 The TOE includes both physical and logical boundaries which are described in Section 1.4 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

8 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:

Figure 1: Logical Boundaries



9 The TOE can be divided into four virtual layers:

a) Basic input/output system (BIOS);

b) Platform and executable module (EM);

c) Security Domain, including Issuer Security Domain and Supplementary Security Domain; and

d) Application.

1.4.2 Physical Boundaries

10 The TOE consist of the following:

Table 3: Physical Components of TOE

Item	Description	Format	Delivery Method	Delivered By
1.	ST31G480 integrated circuit (IC) revision C01.1 ([ST31G_ST])	Water or Module	Courier delivery	STMicroelectronics
2.	MOS Functional Specifications ([MOS_FSP])	PDF	Encrypted Email	MCS
3.	MOS Early Lifecycle Manager Functional Specifications ([MOS_ELM])	PDF	Encrypted Email	MCS

4.	MOS User Guidance ([MOS_UGD])	PDF	Encrypted Email	MCS
5.	Pre-personalisation Agent Authentication Key	Hex	Encrypted Email	MCS

1.5 Clarification of Scope

11 The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.

12 Section 1.4 of this document describes the scope of the evaluation, which is limited to those claims made in the Security Target (Ref [6]).

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

1.6 Assumptions

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

1.6.1 Environmental assumptions

15 Assumptions for the TOE environment as described in the Security Target (Ref [6]):

a) A.Insp_Sys. Inspection Systems or Global Interoperability

The Extended Inspection System (EIS) for global interoperability includes the Country Signing CA Public Key and implements the terminal part of PACE and/or BAC. EIS supports the Terminal Authentication Protocol v.1 and optionally, all the Inspection Systems can implement Active Authentication.

b) A.Auth_PKI. PKI for Inspection Systems

The issuing and receiving States or Organisations establish a public key infrastructure for card verifiable certificates of the Extended Access Control.

c) A.Passive_Auth. PKI for Passive Authentication

The issuing and receiving States or Organisations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical travel document.

1.7 Evaluated Configuration

16 The TOE is to be configured according to the Preparative Guidance and the Security Target (Ref [6]).

17 The TOE evaluated configuration is defined in section 1.3.3 TOE Life Cycle of the last version of Security Target which indicate that the scope of evaluation of limited to phase 1 and part of phase 2 (i.e. Step 1 to Step 3). This means that, in its evaluated configuration:

a) The TOE has not been pre-personalised;

b) The TOE has not been personalised;

c) The issuer Security Domain and Supplementary Security Domain have not been installed yet; and

d) The MF application and ICAO DF have not been installed yet.

18 The evaluator has verified that the TOE samples are provided in the above-described state. The developer also provided a series of resources required to put the TOE into its operational state, after pre-personalisation and personalisation.

a) A series of scripts, provided as part of ATE assessment evidences that would configure the TOE interfaces and would put the latest version of the ES in the TOE, allowing to install ELM, ISD, SSD, MF and ICAO DF.

b) The required guidance for performing pre-personalisation and personalisation of the TOE provided in user guidance document, Functional Specification and Early Lifecycle Manager Functional Specifications.

1.8 Delivery Procedures

19 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

20 The delivery procedures for security products developed, licensed or sold by MCS, particularly its embedded software for smart card IC are described on the Product Delivery document. Those procedures are divided into:

a) Delivery procedures of security products which take on the form of software.

b) Delivery procedures of security products in physical or hardware form.

1.8.1 Software

21 The security products shall be released by the Technical Manager (MCS) and delivered to the receiving party. Each delivery will be accompanied by an acknowledgement receipt or delivery note which must be signed by the recipient and returned to MCS. It contains the following information:

a) Sender's particulars – personnel name and designation, company name, address and contact information.

b) Recipient's particulars – personnel name and designation, company name, address and contact information.

c) Identification of the elements under delivery – description, document name, version number, quantities, etc.

22 The delivery channels are listed here:

a) Email;

b) Company FTP server (MCS or recipient); and

c) Third-party file upload website.

23 The security products will be encrypted with the recipient's PGP key and signed by the Technical Manager or the Engineer authorised to transmit the data. These measures protect the data against disclosure and modification.

24 In the event where the data was uploaded to a server, it will removed from the server immediately after the receiving party has downloaded the data or, at the latest, after five working days. Recipients who do not have a PGP encryption tool may obtain the GNU Privacy Guard (GnuPG) tool from https://www.gpg4win.org/indec.html.

1.8.2 Hardware

25 According to MCS information security policies, a Confidentiality Agreement must be established between MCS and the receiving company before any hardware product may be delivered.

26 The security products shall be released by the Technical Manager and delivered to the receiving party. Each delivery will be accompanied by an acknowledgement receipt or delivery note which must be signed by the recipient and returned to MCS. It contains the following information:

a) Sender's particulars – personnel name and designation, company name, address and contact information.

b) Recipient's particulars – personnel name and designation, company name, address and contact information.

c) Identification of the elements under delivery – description, item name, part number, version number, quantities, etc.

27 The delivery channel listed below:

a) Express courier services, e.g. DHL, NationWide

b) Registered post, e.g. PosLaju

c) Hand delivery by MCS personnel direct to receiving party

28 Documents and small items will be sealed in an envelope with MCS company letterhead. Bigger items will be put into a box and sealed with tamper-evident, security tape which is stamped with MCS company logo and signed and dated by the Technical Manager. The recipient will be able to check the envelope and tape to determine if they were tampered with.

29 Hardware products will be packed according to industry-standard practice to prevent a damage during storage and handling, such as using packaging materials for electrostatic discharge (ESD) sensitive devices, soft foam and bubble wrap, original packing boxes, humidity stickers and so forth.

2 Evaluation

31 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 4 Augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5. The evaluation was performed conformant to the ISCB Product Certification Schemes Policy (Product_SP) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

33 The requirements of [CEM] for the ALC class for an EAL 4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 evaluation level was assessed by the evaluators, analysing the TOE life-cycle documentation provided by the developer. Configuration management, configuration item list, delivery procedures, development security, TOE life-cycle, tools and techniques and composition life-cycle related activities were carried out by the evaluators. Besides, a site audit was conducted in order to determine that those elements were adequately. Besides, a site audit was conducted in order to determine that those elements were adequately being put into practice in the development site of the TOE, which was reported in the report.

34 During the evaluation of the related activities, several issues were raised and reported by the evaluators which were addressed and properly corrected by the developer. Thus, evaluators confirmed that all the requirements in this class were fulfilled and passed.

2.1.2 Development

35 The evaluators assessed the requirements of the ADV class for an EAL 4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 evaluation level of the TOE.

36 During the evaluation of this activity, the security architecture, functional specification, implementation representation and design of the TOE were analyzed and evaluated against the requirements of the CC standard. Several issues were raised and reported by the evaluators, which were addressed and properly corrected by the developer.

37 At the end, the evaluators confirmed that all the requirements for this class were fulfilled and passed.

2.1.3 Guidance documents

38 The evaluators analysed the TOE guidance documentation for secure preparation and installation of the TOE, and the guides for secure operation, provided in MOS User Guidance (Ref [8]).

39 All the evaluation activities for the completion of the class AGD, for the required assurance level, were performed by the evaluator. During the process, several issues were raised and reported by the evaluators, which were addressed and properly corrected by the developer.

40 The evaluators confirmed that the TOE guidance was fulfilled all the requirements and passed for this class.

2.1.4 IT Product Testing

41 Testing at EAL 4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by evaluators from External SEF, JTSEC Beyond IT Security and monitored by Cybersecurity Malaysia MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Report.

2.1.4.1 Assessment of Developer Tests

42 The evaluators verified that the developer has met their testing responsibilities by repeating all the developer test, 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). The results of the evaluators' tests are consistent with the developers' test results defined in their evaluation evidences submitted.

2.1.4.2 Independent Functional Testing

43 At EAL 4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5, independent functional testing is the evaluation conducted by evaluators based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a subset of the developer's test plan, and creating test cases that are independent of the developer's tests.

44 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were recorded by the evaluators and are consistent with the expected test results in the test documentation.

Table 4: Independent Functional Test

Test Suite	Description	Results
Test Suite A1	GET DATA. The main objective of this test is to provide further testing of the entire test plan provided by the developer. The evaluator pretend to test the GET DATA Command in different situations by using all the TSFIs.	Passed. Result as expected.
Test Suite A2	Lifecycle Test. The main purpose of the test is to provide further testing of the different phases of Lifecycle of the TOE. The evaluator will establish the TOE in their state transitions phases and then he will use different functionalities in each application.	Passed. Result as expected.
Test Suite A3	TRNG. The main objective of this test is to verify the TRNG quality.	Passed. Result as expected.
Test Suite A4	Authentication. The main objective of this test is to verify the authentication procedure in its corresponding application. This test suite will use all the TSFIs available.	Passed. Result as expected.
Test Suite A5	Key Storage. The main objective if this test is to verify the resistance to buffer overflow attack of key storage feature of TOE.	Passed. Result as expected.
Test Suite A6	Read record processing with LCS Deactivated. The main objective of this test case consists in verifying if any record referenced by P1 and P2 is in record LCS DEACTIVATED, the command is processed with warning.	Passed. Result as expected.
Test Suite A7	Structure selection. The main objective for this test case consist in verifying if several MF Applications may be installed with the same identifier.	Passed. Result as expected.
Test Suite A8	DF name. The main objective of this test case consists in verifying if the TOE can create two DF files with the same name.	Passed. Result as expected.
Test Suite A9	Activation file. The main objective of this test case consists in verifying if the TOE implements the necessary measures in order to protect the integrity of the files.	Passed. Result as expected.

Test Suite	Description	Results
Test Suite A10	CONFIGURE command. The main objective of this test consists in verifying the possibilities offered by the CONFIGURE command of ELM application.	Passed. Result as expected.
Test Suite A11	NV Memory. The main purpose of this test case consists in verifying the TOE behaviour by modifying the non-volatile memory quota.	Passed. Result as expected.
Test Suite A12	Security attribute configuration. This test consists in verifying the TOE behaviour by modifying the security attribute configuration for accessing CPLC data	Passed. Result as expected.
Test Suite A13	Security attribute configuration (2). This test suite consists in verifying the TOE behaviour by modifying the security attribute configuration "requiring authentication" for GET DATA	Passed. Result as expected.
Test Suite A14	PUT KEY. The main purpose of this test suite is to verify the TOE behaviour by modifying the "Lc" field until an error is caused in the PUT KEY command.	Passed. Result as expected.
Test Suite A15	Applications, key reference. The main purpose of this test suite consists in verifying the TOE behaviour by changing the key reference when there are several applications installed at the same time.	Passed. Result as expected.
Test Suite A16	SCP. The objective of this test suite consists in verifying the TOE behaviour by changing parameters of the SCP protocol.	Passed. Result as expected.
Test Suite A17	SCP termination. The main purpose of this test suite consists in terminating a Secure Channel session by using several applications installed in the TOE.	Passed. Result as expected.

Test Suite	Description	Results
Test Suite A18	Card Content Management. This test suite consists in verifying the TOE behaviour by changing parameters of the Application AID in each installed application.	Passed. Result as expected.
Test Suite A19	Verify the privileges allowed when a new Supplementary Security Domain is installed at the TOE.	Passed. Result as expected.
Test Suite A20	Terminated status. The main purpose of this test suite consists in verifying the TOE behaviour when a state transition to TERMINATED occurs.	Passed. Result as expected.
Test Suite A21	Store feature. The main objective of this test suite consists in verifying the TOE behaviour when there are stored a big amount of data objects.	Passed. Result as expected.
Test Suite A22	Incorrect security condition. The main purpose of this test suite consists in verifying the TOE behaviour when there is an incorrect security condition in the transparent EF creation.	Passed. Result as expected.
Test Suite A23	The main purpose of this test is to create a cyclic structure full of record in order to verify the behaviour of the TOE when a new record is added in the mentioned structure.	Passed. Result as expected.
Test Suite A24	Keys. The main objective of this test to verify the TOE behaviour when there are several keys (with double and triple length) loaded.	Passed. Result as expected.
Test Suite A25	AES keys. The main objective of this test is to verify the TOE behaviour when there are several AES keys (with 32 bytes or more) loaded.	Passed. Result as expected.

Test Suite	Description	Results
Test Suite A26	PSO. The main purpose of this test suite is to check the TOE behaviour when there is an empty buffer during a PSO operation.	Passed. Result as expected.
Test Suite A27	Password Authentication. This test consists in checking the TOE behaviour when the retry counter reset is too long.	Passed. Result as expected.

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

2.1.4.3 Vulnerability Assessments, Penetration Test and/or Analysis

46 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.

47 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks 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 (knowledge of the TOE);

d) Window of opportunity; and

e) Time taken to identify and exploit (elapse time);

f) Specialist technical expertise required (specialised expertise);

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

h) Window of opportunity; and

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

48 By taking into account the mentioned considerations, the vulnerability assessment followed an approach based on two aspects:

a) A code security review, where the evaluators reviewed the source code of the TOE in search potential vulnerabilities.

b) The developers designed and conducted a penetration testing plan based on the Software Attacks methodology described in [JIL_AP].

2.1.4.3.1 Code Security Review

49 The evaluators performed a vulnerability analysis based on an extensive review of the source code, in search of security flaws or defect that could result in potential vulnerabilities. Based on the security issues found, the evaluators provided an analysis of the potential vulnerabilities, for those vulnerabilities detected in the product that could be exploitable by some of the attacks defined in [JIL_AP].

50 Each of the security issues found during the vulnerability assessment based on source code review was reported to the developer which applied the appropriate fixes in the latest version of the TOE.

2.1.4.3.2 Penetration testing

51 The evaluators designed and implemented an AVA penetration testing plan following the methodology described in [JIL_AP] for software attacks applied to smartcards. The penetration tests focused on:

a) Information gathering attacks

b) Editing commands

c) Direct protocol attacks

d) Man-in-the-middle attacks

e) Replay attacks

f) Bypass authentication or access control attacks

g) Buffer overflow or stack overflow attacks

52 The results of the penetration testing demonstrate that the TOE is resistant to an attacker possessing a high attack potential. However, it is important to ensure that the TOE is use only in its evaluated configuration and in a secure environment as specified in the Security Target (Ref [6]).

2.1.4.4 Testing Results

53 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. Therefore, the certifiers confirmed that all the test conducted were PASSED as expected.

3 Result of the Evaluation

54 After due consideration during the oversight of the execution of the evaluation by the certifiers (including development site visit at MCS Office) and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of ePassport Application on MOS version 1.0.0 which is performed by External SEF, JTSEC Beyond IT Security, monitored by Cybersecurity Malaysia MySEF.

55 Cybersecurity Malaysia MySEF found that ePassport Application on MOS version 1.0.0 upholds the claims made in the Security Target (Ref [6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5

56 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. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

57 EAL 4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and complete interface specifications, guidance documentation and a description of the design of the TOE and the implementation to understand the security behaviours.

58 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and independent vulnerability analysis demonstrating resistance to penetration attackers with a high attack potential.

59 EAL 4 augmented ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 also provides assurance through use of development environment controls and comprehensive TOE configuration management including complete automation and evidence of secure delivery procedures.

60 EAL 4 augmented ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 also represent a meaningful increase in assurance by requiring more comprehensive analysis, a structured representation of the implementation, more comprehensive independent vulnerability analysis, and improved configuration management and development environment controls.

3.2 Recommendation

61 The Malaysian Certification Body (MyCB) is strongly recommended that the potential consumer of the TOE are strictly to follow the security recommendations that can be found on the MOS User Guidance (Ref [8]), as well as to observe the operational environment requirements and assumptions defined in the applicable Security Target (Ref [6]).

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July, 2014.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[3] The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[4] ISCB Product Certification Schemes Policy (Product_SP), v1b, CyberSecurity Malaysia, March 2018.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v1a, March 2018.

[6] Security Target of E-Passport Application on MOS v1.0.0, Version 1.0.0, 26 February 2019.

[7] ePassport Application on MOS v1.0.0 Evaluation Technical Report, Version 1.2, 21 March 2019.

[8] MOS User Guidance, Version 1.0.0, 26 February 2019.

A.2 Terminology

A.2.1 Acronyms

Table 5: 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 Organisation for Standardization
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

Acronym	Expanded Term
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 6: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
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. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
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.
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.

--- END OF DOCUMENT ---