MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity
MALAYSIA

C086 Certification Report

Datasonic Chip Operating System (DCOS) version 1.0

File name: ISCB-3-RPT-C086-CR-v1
Version: v1
Date of document: 2 May 2019
Document classification: PUBLIC

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

C086 Certification Report

Datasonic Chip Operating System (DCOS) version 1.0

2 May 2019
ISCB Department

CyberSecurity Malaysia

Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya, Selangor, Malaysia
Tel: +603 8800 7999 Fax: +603 8008 7000
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C086 Certification Report
DOCUMENT REFERENCE:	ISCB-3-RPT-C086-CR-v1
ISSUE:	v1
DATE:	2 May 2019

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
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 2 May 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	12 April 2019	All	Initial draft
v1	24 April 2019	All	Final version

Executive Summary

The Target of Evaluation (TOE) is the Datasonic Chip Operating Chip (DCOS) version 1.0. The TOE is a smart card operating system purpose-designed for national identity card applications which also serves as a platform for national e-passport, precisely meeting individuals needs of countries adopting the latest ID and e-passport standards.

The TOE simultaneously supports multiple applications with custom instruction sets and custom data structures define by the authorized agencies within a single smart card, limited only by the IC specifications. Consider a national ID card with the capabilities of hosting of generic application such as driver's license, e-purse, and bank card credentials, in which simplifies its cardholder's in dealing with various public and private agencies.

The main features are providing secured data accessibility and storage for identity card purpose, provide cryptographic processing (e.g encryption, decryption, key signing and relevant functions), store identity information of the cardholder, support financial trading authentication and record. Additionally, complies to BAC and EAC of ICAO 9309 standard for e-passport.

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 and ALC_FLR.2. 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 Securelytics SEF and the evaluation was completed on 10 April 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 Datasonic Chip Operating Chip (DCOS) version 1.0 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 decide whether to purchase the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The TOE is a Multi-application Smart Card Operating System is composed of hardware and software components. The TOE operates as a platform that store cardholder credentials as definitive electronic national identity card in which serves as national e-passport. The operating system is a native design platform that is using proprietary set of programming structures, in serving as national identity card.

2 The TOE as smart card operating system uses customize command sets (APDU) in communication with the smart card reader (also known as terminal reader or card acceptance device (CAD)), that enables layers of security protection in reading protected data inside the smart card chip memory.

3 Within the design of the smart card chip (IC), the following is the high level structure of the DCOS illustrate in the figure below, with the highlight of the TOE scope of evaluation. Note that the highlight dotted RED line (DCOS Operating System) is the scope of the TOE.

Figure 1: TOE Scope

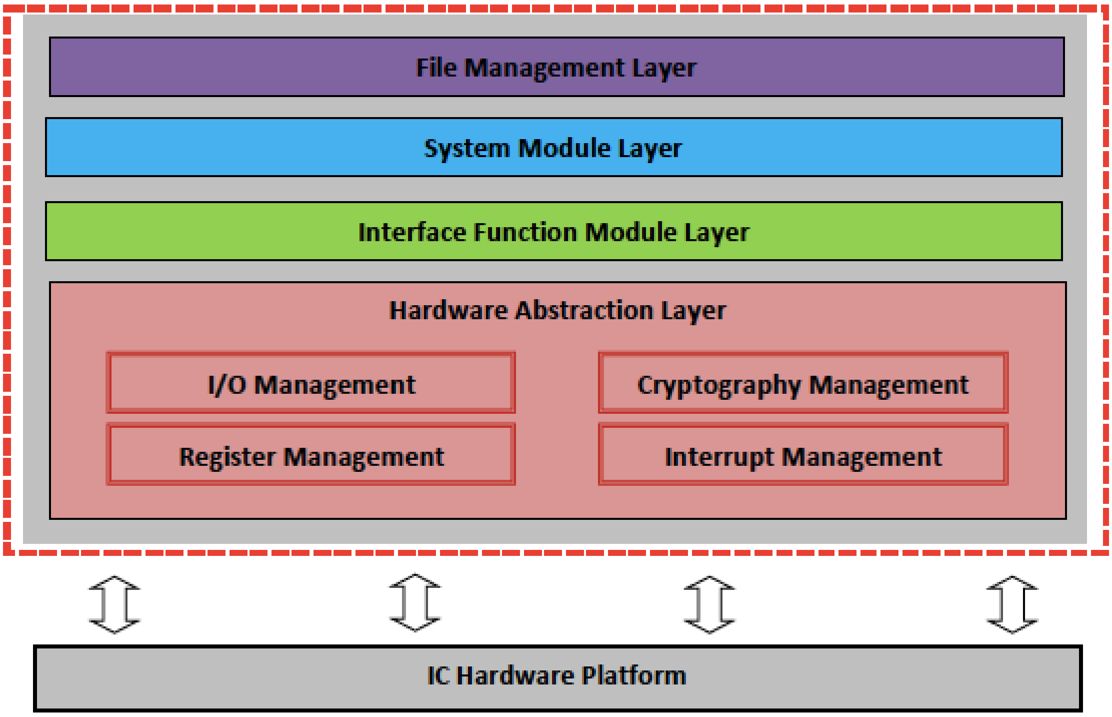


Table 1: List of Components in the TOE Scope

Components	Descriptions
File Management Layer	The File Management Layer holds the data and operations of generic applications by providing those generic applications to load via the virtual machine interfaces platform. Thus, allowing certain runtime API calls by those generic applications using such functions: cryptographic processing, input/output and other programming interfaces.
System Module Layer	The System Module Layer managed the process flow of the TOE by managing the initialization of the TOE and relevant generic applications when being calls in retrieving relevant data related to the generic application management.
Interface Function Module Layer	The Interface Function Module Layer is the TOE component that handles the processing requests between Application Layers and Hardware Abstraction Layer (HAL). Whilst, managing the security functions between layers of data transacted, such as between HAL and the Application Layers.
Hardware Abstraction Layer (HAL)	The hardware Abstraction layer provides access to low level IC routines provided by the certified IC and IC libraries. i. I/O Management; ii. Register Management; iii. RNG & DES Management; and iv. Interrupt Service.

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	C086
TOE Name	Datasonic Chip Operating System (DCOS)
TOE Version	1.0
Security Target Title	DCOS Security Target
Security Target Version	1.0
Security Target Date	9 April 2019
Assurance Level	Evaluation Assurance Level 4 augmented with with ALC_DVS.2 and ALC_FLR.2
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	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL 4 Augmented with ALC_DVS.2 and ALC_FLR.2
Sponsor	Datasonic Smart Solutions Sdn Bhd
Developer	Datasonic Smart Solutions Sdn Bhd
Evaluation Facility	Securelytics SEF

1.3 Security Policy

5 No organisational security policies have been defined regarding the use of the TOE.

1.4 TOE Architecture

6 The TOE includes both physical and logical boundaries which are described in Section 1.5 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

7 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) File Management

The TOE has the capabilities of preventing generic application from interfering with the other generic applications in the aspects of applet execution and accessing private data and operation of the TOE itself.

b) Generic Application and Platform Management

The TOE provides functions of secure installation and secure removal process flow of the generic application by ensuring the data management and processing of the smart card applications are allocated accordingly inside the memory of the smart card chip.

Nonetheless, the platform itself allows the owner of the card lifecycle manage the smart card through its operating system (TOE) in ensuring the continuous of the smart card usage throughout its lifecycle by the cardholder via card services management/revocation.

Additionally, the platform allows the smart card owner to initiate any data/generic application accessibility through secure channel via cryptographic processing.

c) Cryptographic Management

As the smart card chip (IC) has cryptographic functions, this allows the TOE to initiate cryptographic processes on the relevant generic applications, in which these generic applications implement specific security mechanism on top of the evaluated TOE platform.

Note that, the generic applications are not part of the TOE scope of evaluation.

d) TOE Self Protection and Testing

As the platform that manage those generic applications, the TOE requires to provide secure operational environment for those generic applications. Thus, set of triggers that able to react and response to any external events related to smart card chip are required to detects

1.4.2 Physical Boundaries

8 The TOE is a multi-purpose smart card operating system that runs/execute within the hardware operational environment of certified Common Criteria IC hardware platform. Thus, it is been known that the IC hardware platform provides the physical interfaces of the TOE between cardholder with authorized terminal/smart card reader and the data resided in the management of the TOE. Note that the IC hardware platform of the certified Common Criteria, is not included inside the scope of the TOE.

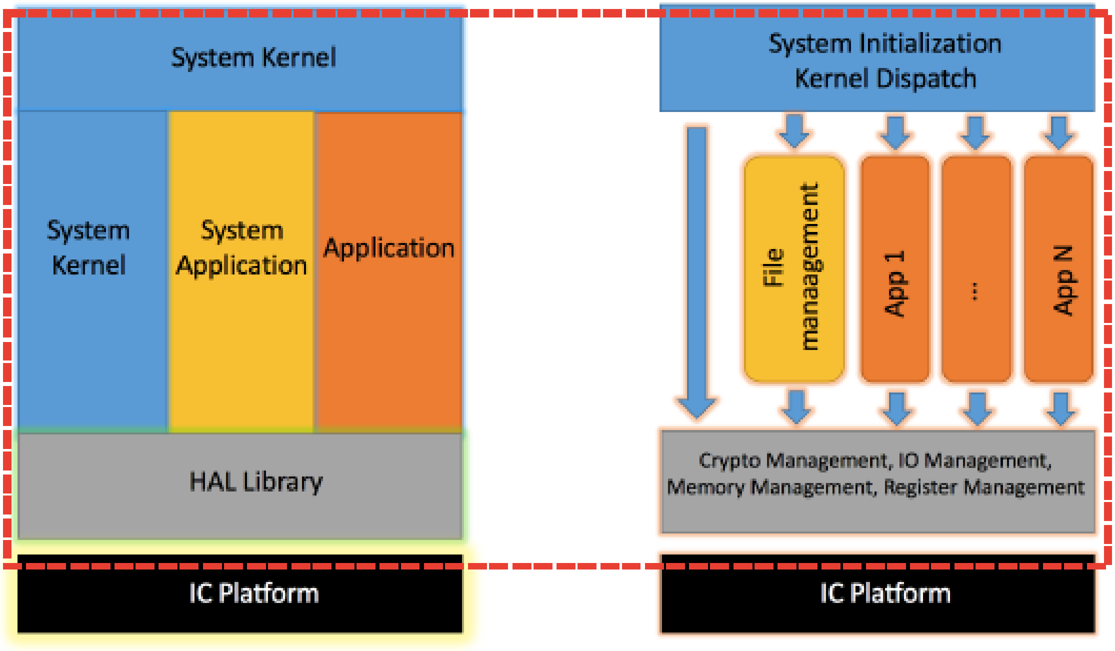
9 In accessing the data or card holder credentials inside the smart card memory, an authorized smartcard reader/terminal reader (also known as Card Acceptance Device, CAD) are required to initiate the request as in between platform of accessibility

between card holder and smart card. Thus, note that the smart card reader/terminal reader (also known as CAD) are not part of the scope of the TOE.

10 Furthermore, the data reside in the smart card memory are under management of the TOE, based on the smart card application access control through certain addressing of the data structures. Thus, it is required to have authorized access control commands known as Application Protocol Data Unit (APDU). The TOE uses APDU commands based on ISO/IEC 7816 and ISO/IEC 14443 requirements as well as there are additional APDU commands design only for specific data structure in the management of the TOE towards the generic applications, known as proprietary APDU commands. On that note, the APDU commands are not part of the TOE.

11 The following is the operations of the TOE illustrated in the figure below. The dotted RED define the boundary of the TOE operations.

Figure 2: TOE Physical Boundaries



1.5 Clarification of Scope

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

13 Section 1.4.3 of this document describes the scope of the evaluation, which is limited to those claims made in the Security Target (Ref [6]).

14 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

15 This section summarizes 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

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

a) A.HW_IC

Assuming that the TOE shall be execute under the platform of certified common certified common criteria hardware platform with the minimum requirements of EAL4 evaluated configurations.

b) A.SEC_DEV

Assuming that the Loaded Applet Developers and Embedded Software Developer shall design the relevant components related to the TOE operations by using authorize software development tools (compliers assemblers, linker, simulators) and software hardware integration testing tools (emulators) that will ensure the integrity of the program and data.

c) A.DELL_APP

Assuming that all relevant generic application shall be removed from the TOE management via the approval and authorization by the card issuer with follow the endorsed administrator guidance.

d) A.USE_TEST

Assuming that the TOE and its relevant components are being tested on the scope of functionality test using a proper process and procedures.

e) A.READER

Assuming that there are secure communications protocols and procedures are used between smart card reader/terminal (CAD) and smart card.

f) A.LOAD APP

Assuming that all relevant generic application shall be loaded to the TOE management are approved and authorized by the card issuer with follow the endorsed administrator guidance.

1.7 Evaluated Configuration

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

18 The scope of the TOE only covers the Operating System of the Smart Card Chip and generic applications.

19 The list of IC hardware platforms are not part of the scope of the TOE, and shall not be re-evaluate in this scope of the TOE.

20 List of IC Model Supported by the TOE:

a) Infineon

b) NXP

21 In the TOE operational environment, the following is the list of components consist of hardware and software that composing the TOE, in which defined as non-dependencies to the TOE

a) IC Hardware

b) Dedicated software

c) Operating system (which is as part of TOE

d) Generic applications System Interface (which is as part of TOE)

e) Generic applications

1.8 Delivery Procedures

22 The evaluators examined the delivery procedure, in which provide guidance for the developer to initiate delivery process of the TOE and its components to the intended recipient(s). It is also provide direction on the methods used to deliver the TOE to consumers and users of the product.

23 To ensure that the TOE being delivered securely upon its

a) When the order is taken, Developer will send the encrypted release note to intended recipient (customer, end-user or etc.) by email for the release information (Product Name, version and customer ID)

b) Schedule is given out to intended recipient (customer, end-user or etc.) regarding the delivery of the TOE so that intended recipient (customer, end-user or etc.) can know when is the TOE is expected to be delivered by representative of Developer via email or phone call

c) A compressed and encrypted archive containing the TOE or packaged in form of physical smartcard or relevant forms agreed by intended recipient (customer, end-user or etc.) is produced by Developer and will be securely packaged in a box with seal;

d) The seal packaging securely will then be sent to the intended recipient (customer, end-user or etc.).

24 Upon received of the TOE in form of agreed by the recipient, the relevant parties required to sign and perform checking on the checklist provided by developer. The form checklist shall be signed as acknowledgement of the received products as well as shall be returned back to developer. Submission can be performed via email, postage and fax.

1.8.1 Software

25 The TOE is in forms of software and relevant digital formats that is applicable to be transmitted over the Internet using forms of secure packaging or secure data packaging with applied additional layers of security. The TOE consists of data or binary will be ZIP and encrypted using PGP format keys signed with public keys of the recipient Person in Charge (PIC) and private key of the TOE Developer Person in Charge (PIC).

26 Likewise, alternative platform that the PGP usage are not permitted, the data transmitted shall be ZIP protected with PIN/Password created by the TOE Developer PIC. The data and the PIN/Password will be delivered using different platform to mitigate issue of information sniffing, such as that the ZIP data protected with PIN/password will be send using email or provided link (secure channel download link) and the PIN/password will be send through SMS or phone call.

1.8.2 Physical document

27 As for physical document and small items will be sealed in an enveloped or packaging box with developer company letterhead.

28 Bigger items will be put into a box and seal with tamper-proof security tape which is stamp with the TOE developer logo. The box will be labelled with sticker that shall be signed by Technical Manager of the developer as proof of product released to another authorized party(s). Inside the envelop or box shall be a delivery note requires by the

TOE recipient to signed and email back to TOE developer as acknowledgement of received.

29 Under certain condition the TOE need to be delivered by hand directly to the external parties such as ICC manufacturer or card manufacturer, these requires authorization engagement made between TOE developer and the recipient.

2 Evaluation

30 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 and ALC_FLR.2. 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

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

2.1.1 Life-cycle support

32 The requirements of [CEM] for the ALC class for an EAL 4 augmented with ALC_DVS.2 and ALC_FLR.2. 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 model, development tools and flaw remediation activities were carried out by the evaluators. Besides, a site audit was conducted in order to determine that those elements were adequately. 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.

33 Evaluators confirmed that all the requirements in this class were fulfilled and passed.

2.1.2 Development

34 The evaluators assessed the requirements of the ADV class for an EAL 4 augmented with ALC_DVS.2 and ALC_FLR.2 evaluation level of the TOE.

35 During the evaluation of this activity, the security architecture, functional specification, implementation representation and TOE design were analyzed and evaluated against the requirements of the CC standard.

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

2.1.3 Guidance documents

37 The evaluators analyzed the TOE guidance documentation for secure preparation and installation of the TOE, and the guides for secure operation, provided in User Guide (Ref [8]).

38 Evaluator examined operational user guidance and preparative procedures.

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

2.1.4 IT Product Testing

40 Testing at EAL 4 augmented with ALC_DVS.2 and ALC_ FLR.2 consists of assessing developer tests, sufficiency test and conducting penetration tests. The TOE testing was conducted by evaluators from Securelytics SEF. 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

41 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 Testing Sufficiency

42 At EAL 4 augmented with ALC_DVS.2 and ALC_FLR.2, testing sufficiency demonstrates the correspondence between the security functional requirements (SFRs) defined in Security Target, and the test cases that test the functions and behaviour of the TOE that meets those requirements. The evaluators have decided to perform testing based on the TOE Security Functions.

43 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 3 below provides an overview of the evaluators test and provides a mapping to the relevant security functional requirements that were exercised during the testing effort.

Table 3: Testing Sufficiency

Test ID	Description	SFRs	Results
F001	Cryptographic Operation & Generation To test that the TOE performs 3DES cryptographic operation	FCS_COP.1, FCS_CKM.1	Pass
F002	Cryptographic Operation & Generation To test that the TOE performs RSA cryptographic operation	FCS_COP.1, FCS_CKM.1	Pass
F003	Cryptographic Operation & Generation To test that the TOE performs ECC, SHA-256 & SHA-1 cryptographic operation	FCS_COP.1, FCS_CKM.1	Pass
F004	Access Control Function The TOE shall enforce the Lifecycle Management SFP to objects during the card initialisation	FDP_ACF.1, FDP_ACC.2	Pass
F005	Access Control Function Authenticating Open Card Key during initialization	FDP_ACF.1	Pass
F006	Access Control Function MyKad personalisation (anti tearing), Applet loading and deletion	FIA_ATD.1	Pass
F007	User Data Protection, Security Management BR Test – unconditional (Ins 00h)	FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FRU_RSA.1	Pass
F008	User Data Protection, Security Management JPSLE Test – conditional (Ins 1Ah)	FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FRU_RSA.1	Pass
F009	User Data Protection, Security Management PUSH:B:I:P Test (Ins 7Eh).	FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FRU_RSA.1	Pass

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

2.1.4.3 Vulnerability Analysis

45 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.

46 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) Equipment

47 The developers search for vulnerabilities also considered public domain sources for published vulnerability data related to the TOE and the contents of all TOE deliverables. The source of research as stated below:

a) Reference Book

- Power Analysis Attacks, Revealing the Secrets of Smart Card by Stefan Mangard, Elisabeth Oswald and Thomas Popp, Springer Publication 2007
- Smart Card Applications, Design Models for using and programming smart cards by Wolfgang Rankl, Wiley Publication 2007

b) Reference publication paper

- Design and Setup of Power Analysis Attacks, by Mariana Safta, Paul Svasta, Mihai Dima and Andrei Marghescu, 2016 IEEE Publication.
- Known Attacks Against Smartcards, by Discretix Technologies Ltd, Whitepaper publication.
- Power Analysis Attack: A vulnerability to Smart Card Security, by Hridoy Jyoti Mahanta and Abdul Kalam, Ajoy Kumar Khan, SPACES 2015 Publication

2.1.4.3.1 Vulnerability testing

48 The penetration tests focused on:

a) Simple Power Analysis (SPA) Attack

b) Differential Power Analysis (DPA) Attack

49 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

50 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

51 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 Datasonic Chip Operating System (DCOS) version 1.0 which is performed by Securelytics SEF.

52 Securelytics SEF found that Datasonic Chip Operating System (DCOS) version 1.0 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 and ALC_FLR.2

53 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

54 EAL 4 augmented with ALC_DVS.2 and ALC_FLR.2 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.

55 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.

56 EAL 4 augmented ALC_DVS.2 and ALC_FLR.2 also provides assurance through use of development environment controls and comprehensive TOE configuration management including complete automation and evidence of secure delivery procedures.

57 EAL 4 augmented ALC_DVS.2 and ALC_FLR.2 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

58 The Malaysian Certification Body (MyCB) is strongly recommended that:

a) The users should make themselves familiar with the developer guidance provided with the TOE, pay attention to all security warnings as well as to observe the operational environment requirements and assumptions defined in the applicable security target.

b) The users must maintain the confidentiality, integrity and availability of security relevant data for TOE initialization, start-up and operation if stored or handled outside the TOE.

c) System Auditor should review the audit trail generated and exported by the TOE periodically.

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 DCOS, Version 1.0, 9 April 2019.

[7] Evaluation Technical Report - DCOS Version 1.0, 10 April 2019.

[8] DCOS User Guidance, Version 1.0, 8 Mar 2019.

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 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
PP	Protection Profile

Acronym	Expanded Term
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 5: 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.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.

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

--- END OF DOCUMENT ---