C006 Certification Report

MCS Small Machine Operating System CC (SMOSCC) v1.0.0

File name: ISCB-5-RPT-C006-CR-v1a
Version: v1a
Date of document: 25 September 2012
Document classification: PUBLIC

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

C006 Certification Report

MCS Small Machine Operating System CC (SMOSCC) v1.0.0

25 September 2012

ISCB Department

CyberSecurity Malaysia

Level 8, Block A, Mines Waterfront Business Park,

No 3 Jalan Tasik, The Mines Resort City

43300 Seri Kembangan, Selangor, Malaysia

Tel: +603 8946 0999 Fax: +603 8946 0888

http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C006 Certification Report - MCS Small Machine Operating System CC (SMOSCC) v1.0.0
DOCUMENT REFERENCE:	ISCB-5-RPT-C006-CR-v1a
ISSUE:	v1a
DATE:	25 September 2012

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

The copyright of this document, which may contain proprietary information, is the property of CyberSecurity Malaysia.

The document shall be held in safe custody.

©CYBERSECURITY MALAYSIA, 2012

Registered office:

Level 8, Block A,

Mines Waterfront Business Park,

No 3 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 25 September 2012, 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.

Reproduction of this report is authorized 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 (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 Revision 3 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 Revision 3 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
v1	13 September 2012	All	Final Released.
v1a	25 September 2012	Page iv	Add the date of the certificate.

Executive Summary

Small Machine Operating System – Common Criteria or SMOSCC version 1.0.0 is a multi-application smart card integrated circuit (IC) operating system purpose-designed for national ID applications which also serves as an ideal platform for national e-passport. SMOSCC from MCS Microsystem Sdn Bhd is the Target of Evaluation (TOE) for Evaluation Assurance Level (EAL) 4 augmented with ALC_DVS.2 and ALC_FLR.1 evaluation.

SMOSCC simultaneously supports multiple custom applets with custom instruction sets and data structures from several agencies on a single smart card, limited only by the IC specification. Consider a national ID card with a host of other functions like driving license, PKI token, e-purse, and frequent traveller which will simplify the cardholder's dealings with various private and public agencies.

The TOE includes an instruction agnostic virtual machine environment capable of providing a portable interface for smart card applications. It also provides several libraries providing hardware IC services such as cryptography to third party applications.

The TOE implements the following components that reside upon hardware platform IC as mention below:

- Small Machine - To implement a virtual machine to run loaded application and runtime API.
- Early Lifecycle Manager - Used during the first phases of the TOEs lifecycle in order to commence the setup of the TOE.
- SMOS Card Manager - Used once the TOE is an initialised state and manages the installation and removal of loaded applications and the SMOS card lifecycle.
- Hardware Abstraction Layer - To provide access to low level IC routines.

The security function within the scope of TOE includes:

- Application Firewall - To prevent applications from interfering with the execution and private data of other loaded applications and the operation of the TOE itself.
- Application and Platform Management - To provide functionality for managing the secure installation/removal of loaded applications and enforcing its lifecycle.
- Cryptographic Management - To utilise cryptographic mechanism in order to enforce the remaining TOE security functions.
- TOE Self Protection and Testing - To provide a secure environment on which to host loaded applications. The TOE protects itself from physical tampering attacks and hardware failures by working in conjunction with its underlying hardware platform.

The TOE runs on a Common Criteria certified smart card IC hardware platform specified in Section 1.4 of the Security Target (Ref [6]). However, the underlying IC hardware platform, card acceptance devices and loaded applications (applets) are not part of the TOE. It communicates with card acceptance devices which exist within the environment,

and supports ISO/IEC 7816 contact based, and ISO/IEC 14443 contactless based card acceptance devices.

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

This report confirms the findings of the security evaluation of SMOSCC to the Common Criteria (CC) evaluation assurance level EAL4 augmented with ALC_DVS.2 and ALC_FLR.1. The report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]). The evaluation was performed by CyberSecurity Malaysia MySEF and completed on 1 August 2012.

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

It is the responsibility of the user to ensure that the SMOSCC meets their requirements and security needs. It is recommended that a potential user of the SMOSCC 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), MCS Small Machine Operating System CC version 1.0.0 (hereafter referred as SMOSCC) is a multi-application smart card integrated circuit (IC) operating system purpose-designed for national ID applications. It supports multiple customs applets on a single smart card, limited only by the IC specifications. Consider a national ID card with a host of other functions like driving license, PKI token, e-purse, and frequent traveller which will simplify the cardholder's dealings with various private and public agencies.

2 The TOE includes an instruction agnostic virtual machine environment capable of providing an interface for smart card applications. It also provides several libraries providing hardware IC services such as cryptography to third party applications.

3 SMOSCC consist of the following components:

a) Small Machine - The heart of the system which implements a virtual machine to run loaded applications.

b) Early Lifecycle Manager - To be used during the first phases of the TOEs lifecycle.

c) SMOS Card Manager - It is used once the TOE is in an initialised state and manages the installation and removal of loaded application. (i.e. applets)

d) Hardware Abstraction Layer - To provide access to low level IC routines provided by the certified IC. It is like an interface for Small Machine to communicate with Smart Card IC. Note: Smart Card IC is not part of the TOE scope.

4 The security functions that within the scope of TOE includes:

a) Application Firewall - To prevent applications from interfering with the execution from other loaded applications and the operation of the TOE itself.

b) Application and Platform Management - To provide functionality for managing the secure installation/removal of loaded applications and enforcing its lifecycle.

c) Cryptographic Management - To utilised cryptographic mechanism in order to enforce the remaining TOE security functions.

d) TOE Self Protection and Testing - To provide a secure environment on which to host loaded application. The TOE protects itself from physical tampering attacks and hardware failures by working in conjunction with its underlying hardware platform.

5 The TOE runs on a Common Criteria certified smart card IC hardware platform specified in Section 1.4 of the Security Target (Ref [6]). However, the underlying IC hardware platform, card acceptance devices and loaded applications (applets) are not part of the TOE. It communicates with card acceptance devices which exist within the

environment, and supports ISO/IEC 7816 contact based, and ISO/IEC 14443 contactless based card acceptance devices.

1.2 TOE Identification

6 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C006
TOE Name	MCS Small Machine Operating System CC (SMOSCC)
TOE Version	1.0.0
Security Target Title	MCS Small Machine Operating System CC Security Target
Security Target Version	1.0.0
Security Target Date	29 December 2010
Assurance Level	EAL4+ ALC_DVS.2 and ALC_FLR.1
Criteria	Common Criteria for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3 (Ref [2])
Methodology	Common Evaluation Methodology for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC part 2 conformant CC part 3 conformant Package conformance to EAL4 augmented with ALC_DVS.2 and ALC_FLR.1
Sponsor and Developer	MCS Microsystems Sdn Bhd 4th Floor, IRIS Smart Technology Complex, Technology Park Malaysia, Bukit Jalil,57000 Kuala Lumpur
Evaluation Facility	CyberSecurity Malaysia MySEF

1.3 Security Policy

7 SMOSCC implements access control policy to restrict the ability of authorised user to access the system. Early Lifecycle Manager will enforce Lifecycle Management Policy on user that attempt to retire the card from an initialize state. In order to change the security attributes of an initialized card, the card issuer must authenticate cryptographically.

8 SMOSCC does not permit one loaded application from interfering with the operation of behaviour of another loaded application or by TOE itself. This can be achieved by enforcing the Inter-Loaded-Application Firewall policy.

9 The TOE enforces Loaded Application Installation & Removal policy to ensure that only authorised parties can install or remove the applications to or from the IC. Once loaded, the application must be signed by the appropriate cryptographic key defined during the TOE initialisation.

10 The details of access control policy are described in Section 5.6 and Section 6.2 of the Security Target (Refer [6]).

1.4 TOE Architecture

11 Based on Figure 1, SMOSCC architecture is segregated based on several layers that operate accordingly and supported by card acceptance device also known as smart card terminal reader. In general, SMOSCC is the brains of the whole operations illustrated in Figure 1 that perform processing capabilities as an operating system for smart card from all the interfaces surrounding the smart card operational environment.

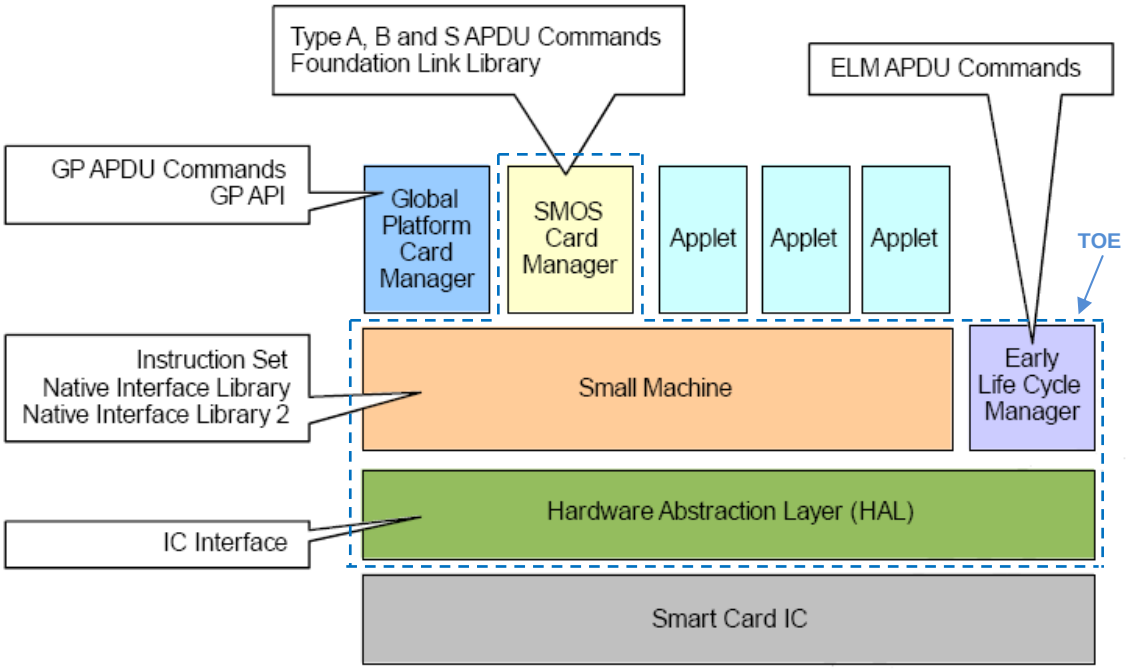

Figure 1: Basic SMOSCC Architecture

12 The TOE runs on a Common Criteria certified smart card IC hardware platform, describes in Section 1.4 of the Security Target (Ref [6]). It is assumed that the underlying IC hardware platform is certified to at least the same assurance level as the TOE including all cryptographic and other support services utilized by the TOE.

13 As described in Section 1.5 of the Security Target (Ref [6]), the TOE operational environment is divided into three categories as follows:

a) TOE Environment.

b) TOE Development Environment

c) TOE User Environment

14 All applets (not part of the evaluation scope) are managed by the TOE via SMOS Card Manager and Global Platform Card Manager supported via several interfaces through Small Machine that will provide interfaces of communications between card acceptance device and smart card hardware.

15 The TOE is a combination of several subsystems as mention below:

a) Small Machine - This is the heart of the system. It implements a virtual machine to run loaded and running applications. Its function is to translate instruction from the applications to other subsystems. It behaves in the same way an ordinary CPU does in that it fetches, decodes, and executes instruction from an instruction pipeline. The interfaces presented in this subsystem are Instruction set, Native Interface Library, and Native Interface Library 2. The Small Machine does not permit loaded applications to perform operations that would interfere with other loaded applications.

b) Early Life Cycle Manager (ELM) - It is used in the first phases of TOE's lifecycle in order to commence the setup of the TOE. By using ELM APDU Commands it helps to initialise data, software configuration, and patch code.

c) Hardware Abstraction Layer (HAL) - It provides access to low level IC routines provided by the certified IC. It uses IC interface which is a logical interface that exist between the SMOSCC operating system (code running on IC hardware) and the IC actually executing the code.

d) SMOS Card Manager - It is used once the TOE is in initialised state. The APDU commands are invoked via a card acceptance device. The interfaces that used to interact with card acceptance devices are Type A APDU Commands, Type B APDU Command, Type S APDU Command, and Foundation Link Library.

1.4.1 Logical Boundaries

16 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) Application Firewall - To prevent applications from interfering with the execution and private data of other loaded applications and the operation of the TOE itself.

b) Application and Platform Management - To provide functionality for managing the secure installation/removal of loaded applications and enforcing its lifecycle. The TOE is flexible in that it provides capability to allow a single owner to control the entire card, including its lifecycle (such as retirement of the card once it's in service) and also support trusted third parties having the capability via cryptographic authentication to remotely load and unload application during the smart card lifetime.

c) Cryptographic Management - To utilise cryptographic mechanisms in order to enforce the remaining TOE security functions. The TOE provides cryptographic functions available to loaded applications. This allows loaded application to

implement their own security mechanisms on top of the evaluated SMOSCC platform. The loaded applications are not part of the evaluation scope.

d) TOE Self Protection and Testing - To provide a secure environment on which to host loaded application. In order to achieve this, the TOE must react and respond to external events such as hardware failure and deliberate attempts to circumvent its security features. Furthermore, the TOE protects itself from physical tampering attacks and hardware failures by working in conjunction with its underlying hardware platform. The underlying hardware platform is not part of the evaluation scope.

17 For more details, please refer to Security Target (Ref [6]), Section 1.5.1.

1.4.2 Physical Boundaries

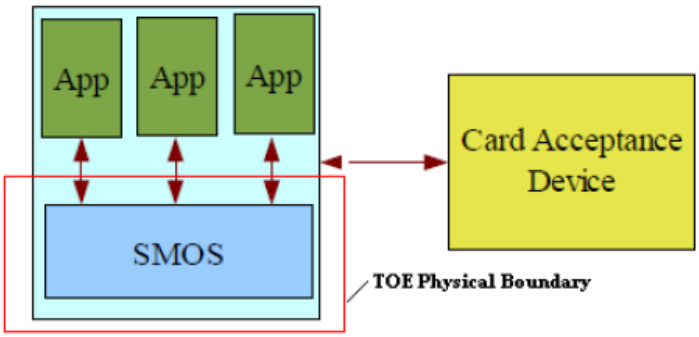

Figure 2: SMOSCC Physical Scope

18 The TOE is masked onto the physical IC hardware platform where it is installed in the IC's memory and is executed using the IC's processor. It is assumed that the TOE runs on a Common Criteria certified smart card IC hardware platform. However, the IC hardware platform, including the IC platform processor, memory, and other components, are not part of the evaluation scope. Table 2 of the Security Target (Ref [6]) describes the lifecycle of the TOE and its relationship with the underlying IC.

19 The TOE communicates with card acceptance devices which exist within the environment. The card support ISO/IEC 7816 contact based, and ISO/IEC 14443 contactless based card acceptance devices. The card acceptance device is not part of the TOE.

20 For more details, please refer to Security Target (Ref [6]), Section 1.5.2.

1.5 Clarification of Scope

21 Section 1.4.1 of this document describes the scope of the evaluation. The scope of the evaluation was limited to those claims made in the Security Target (Ref **Error! Reference source not found.**).

22 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.

23 The scope of the evaluation only includes the libraries of the operating system and loaded-application system interface on the Small Machine virtual machine.

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

a) All underlying IC hardware platform,

b) Dedicated software, and

c) Loaded-applications.

1.6 Assumptions

25 This section summaries the security aspects of the environment/configuration in which the IT product is intended to operate. Consumers should understand their own IT environments that required for secure operation of the SMOSCC defined in subsequence sections and in the Security Target (Ref [6]).

1.6.1 Usage assumptions

26 There is no Assumption for the TOE usage listed in the ST.

1.6.2 Environment assumptions

27 Assumption for the TOE environmental listed in the ST includes:

a) The TOE shall be masked onto a smart card integrated circuit evaluated to at least the same assurance level as the TOE. The scope of the underlying evaluated hardware platform must include all security functionality utilised by the TOE including cryptographic implementation and side channel detection countermeasures. Where a certified IC provides evaluated cryptographic libraries these may be used as an interface from within the embedded software. Where no certified library exists, the embedded software OS will provide the interface as part of the TOE.

b) It is assumed that the TOE material/ information under delivery and storage shall be protected.

c) It is assumed that correct actions shall be taken in the event of improper operation during the delivery process and storage.

d) Those responsible for the application of delivery procedures shall have the required training and expertise.

e) It is assumed that appropriate functionality testing of the TOE is used in phases 3, 4, 5 and 6.

f) It is assumed that security procedures are used during all manufacturing and test operations through phases 3, 4, 5 and 6 to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

g) It is assumed that secure communication protocols and procedures are used between smart card and terminal.

h) Whenever a loaded-application is to be loaded on the platform, it is assumed that its development and production follow the Administrator Guidance.

1.7 Evaluated Configuration

28 This section describes the configurations of the TOE that were included within the scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in the defined evaluated configuration according to the guidance documents specified in Section 1.9 of this document.

29 The TOE is delivered as an application by the developer and the administrator must then configure the TOE accordingly.

30 The TOE process starts with initialisation process which involves card manufacturer. When SMOSCC IC arrives at the card manufacturer, it has limited function as provided by the ELM. This process will then convert SMOSCC from Pre-initialisation to Post-initialisation state. The keys are protected based on TDES cryptography.

31 Personalisation process will take part after card initialisation is done. In this time, SMOSCC is in Post-initialisation state. The SMOS Card Manager is active and all of its functions are available, i.e. Type A, B and S commands. Applets are loaded in the TOE and they are personalised with card holder data. Normally, the personal particulars are printed on the smart card at this time.

32 During Field Usage lifecycle, the SMOSCC smart card has been issued to the cardholder. Its usage is defined by the Applets found on the smart card. Moreover, new Applets may be installed and unused Applets may be removed.

33 The last process of the SMOSCC is the Applet development. Applet providers are responsible for the development of the Applets. They deliver the Applet method, object, and certificate files to the Personaliser to be installed in SMOSCC smart card.

1.8 Delivery Procedures

34 The TOE is sent to the customers using the delivery procedure, which ensures that the TOE is securely transferred from the development environment into the responsibility of the customer.

35 Any software or digital format of the TOE that will be transmitted by the computer to the receiving party must be encrypted by using PGP keys and signed by the Technical Manager or the Engineer authorised to transmit the data.

36 Physical documents, IC wafer and modules, IC cards and inlays, and portable media will be sealed in an envelope with the 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 Technical Manager. The delivery channels are via standards couriers, registered post or hand delivery by MCS personnel.

37 After receiving the package, the customer is instructed (as per guidance document) to verify the integrity of the TOE. Each delivery will be accompanied by an acknowledgement receipt or delivery note, which must be signed by the recipient and returned to MCS. This is achieved using the steps below:

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 and etc.

38 The security products embedded with SMOSCC may be shipped directly from the IC manufacturer to the card manufacturer upon authorisation from MCS.

1.9 Documentation

39 To ensure continued secure usage of the product, it is important that SMOSCC is used in accordance with guidance documentation.

40 The following documentations are provided by the developer for the development of secured loaded applications of the TOE:

a) Migration from SMOS to SMOSCC (SMCC-GD-Migration-1v0v0), version 1.0.0, 29 December 2010.

b) Programmer's Guide (SMCC-GD-ProgrammersGuide-1v0v0), version 1.0.0, 29 December 2010.

c) User Guidance (SMCC-GD-UserGuide-1v0v0), version 1.0.0, 28 December 2010.

41 The following documentations are provided by the developer to the end user as guidance to ensure secure operation of the product:

a) User Guidance (SMCC-GD-UserGuide-1v0v0), version 1.0.0, 28 December 2010.

b) 8001 Release Note (SMCC-GD-8001RelNote-1v3v0), version 1.3.0, 28 December 2010

2. Evaluation

42 The evaluation was conducted in accordance with the requirements of the Common Criteria Version 3.1 Revision 3 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 3 (Ref [3]). The evaluation was conducted at Evaluation assurance Level 4 Augmented with ALC_DVS.2 and ALC_FLR.1. 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

43 The evaluation activities involved a structured evaluation of SMOSCC including the following components:

2.1.1 Life-cycle support

44 An analysis of the SMOSCC configuration management system and associated documentation was performed. The evaluators confirmed that the configuration list which includes the TOE and the evaluation evidence were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items.

45 It is evaluated that the implemented configuration management system can control changes to those items that have been placed under configuration management system. The developer's configuration management system was also observed during the site visit, and it was found security flaws under configuration management ensures that security flaw reports are not lost or forgotten, and allows a developer to track security flaws to their resolution. This is evaluated to be consistent with the provided evidence.

46 During the site visit the evaluators examined the development security documentation and determined that it detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the SMOSCC design and implementation. The evaluators confirmed that the developer used a documented life-cycle model which provides necessary control over the development and maintenance of SMOSCC by using the procedures, tools and techniques described by the life-cycle model.

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

2.1.2 Development

48 The evaluators analysed the SMOSCC functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and modules. The design described the TOE subsystems to sufficiently determine the TSF boundary, and

provides a description of the TSF internals in terms of modules. It provides a detailed description of the SFR-enforcing modules and enough information about the SFR-supporting and SFR-non-interfering modules for the evaluator to determine that the SFRs are completely and accurately implemented.

49 The evaluators analysed the SMOSCC security architectural description and determined that the delivery and installation process was secure and the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

2.1.3 Guidance documents

50 The evaluators examined the SMOSCC 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

51 Testing at EAL4 consists of assessing developer tests, performing independent function test, and performing penetration tests. The SMOSCC testing was conducted by CyberSecurity Malaysia MySEF and at the developer's site where it was subjected to a comprehensive suite of formally documented, and independent functional tests. For the penetration tests, it was conducted by external lab, Witham Lab Australia, under the purview of Stratsec.net Sdn Bhd accredited by NATA (National Association of Testing Authorities, Australia). 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

52 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).

53 The evaluators analysed the developer's test coverage and depth analysis 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 implementation representation, functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

54 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 a sample of the developer's test plan, and creating test cases that augmented the developer tests.

55 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 tests developed and performed by the evaluators to verify the TOE functionality are as follows:

Table 2: List of Evaluator Independent Test

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
A series of test cases on TOE security functions of Application Firewall, which is preventing applications (applets) from interfering with the execution and private data of other loaded application and the operation of the TOE itself.	Application Firewall (AppFW)	Instruction Set Native Interface Library (SYS) Native Interface Library 2 (SYS2) Type B APDU Commands	**PASS**. Result as expected.
A series of test cases on TOE security functions of Application and Platform Management, which is managing the secure installation/removal of loaded applications and enforcing its lifecycle.	Application and Platform Management (SF.Platform AppMgmt)	Instruction Set Native Interface Library (SYS) Native Interface Library 2 (SYS2) Type A APDU Commands Type B APDU Commands Type S APDU Commands Early Lifecycle Manager APDU Commands	**PASS**. Result as expected.
A series of test cases on TOE security functions for Cryptography Management, which is utilise cryptographic mechanism in order to enforce the remaining security functions.	Cryptography Management (SF.Crypto)	Native Interface Library (SYS) Native Interface Library 2 (SYS2) Foundation Link Library (FFL) Type B APDU Commands Type S APDU	**PASS**. Result as expected.

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
		Commands IC Interface	
A series of test cases on TOE security functions for TOE Self Protection and Testing, which is providing a secure environment on which to host loaded applications.	TOE Self Protection and Testing (SF.TstProt)	Type B APDU Commands IC Interface	**PASS**. Result as expected.

2.1.4.3 Penetration Testing

56 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE and to determine whether these were exploitable in the intended operating environment of the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, TOE design, security architecture description, and implementation representation.

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

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

b) Specialist technical expertise required (specialist expertise);

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

d) Window of opportunity; and

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

58 The penetration tests focused on:

a) Correlation Power Analysis (CPA); and

b) Differential Power Analysis (DPA).

59 The results of the penetration testing note that there is no exploitable vulnerability and/or residual vulnerability found that is beyond Basic and Enhanced-Basic attack potential. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment.

2.1.4.4 Testing Results

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

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

3. Result of the Evaluation

62 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 SMOSCC performed by the CyberSecurity Malaysia MySEF.

63 CyberSecurity Malaysia MySEF found that SMOSCC upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) assurance level EAL4+ ALC_DVS.2 and ALC_FLR.1.

64 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 undiscovered in its claimed security functionality. This risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

65 EAL4 provides assurance by a full Security Target (ST) and an analysis of the security functions in the ST, using a functional and complete interface specification, guidance documentation, a description of the basic modular design of the TOE, and a subset of the implementation to understand the security behaviour.

66 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and a vulnerability analysis demonstrating resistance to penetration attackers with an Enhance Basic attack potential.

67 EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.

3.2 Recommendation

68 In addition to ensure secure usage of the product, below are additional recommendations for SMOSCC consumers:

a) For future development and improvement, management of physical TOE on developer site shall be located firmly in dedicated storage room for better management if the TOE goes for mass production/delivery.

b) Implementing digital certificate security in signing all logical data transferred between developer and client are suggested for better verification process. This improvement is meant to replace the current process of acknowledgement notes. Implementation process shall be included with digital certificate validation by Certificate Authority (CA).

c) All guidance and manual shall be followed closely to ensure the secure configuration of 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 3, July 2009.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

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

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

[6] MCS Small Machine Operating System CC Security Target, Version 1.0.0, 29 December 2010

[7] Evaluation Technical Report MCS Small Machine Operating System CC (SMOSCC), Version 1.1, 1 August 2012

A.2 Terminology

A.2.1 Acronyms

Table 3: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CPU	Central Processing Unit
IC	Integrated Circuit
ID	Identity Card
IEC	International Electrotechnical Commission
ISCB	Information Security Certification Body
ISO	International Organisation for Standardization
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme

Acronym	Expanded Term
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
SMOSCC	MCS Small Machine Operating System CC
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS ISO/IEC Guide 65
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained to achieve consistency. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology.
Certifier	The person responsible for managing a specific certification task.
Evaluator	The person 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 the 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 ---