KECS-CR-06-11

Certification Report on MULTOS SM10 R2 of SAMSUNG SDS Co., Ltd.

Certification No. : KECS-ISIS-0051-2006

September 2006

National Intelligence Service
IT Security Certification Center

This document is the certification report on MULTOS SM10 R2 of SAMSUNG SDS Co., Ltd.

Certification Body

National Intelligence Service

Evaluation Body

Korea Information Security Agency

Table of Contents

1. Overview

This report is for the certification body to describe the certification result, which inspects the results of the EAL 4+ evaluation of SAMSUNG SDS Co., Ltd.('SAMSUNG SDS' hereinafter) MULTOS SM10 R2 with regard to the Common Criteria for Information Technology Security Evaluation (Notification No. 2005-25 of the Ministry of Information and Communication; 'CC' hereinafter).

The Korea Information Security Agency (KISA) has evaluated SAMSUNG SDS MULTOS SM10 R2, and finished the evaluation on the 9th of August, 2006. This report is written based on the Evaluation Technical Report produced and provided by the KISA. The evaluation concludes that the TOE satisfies the CC V2.3 part 2 and EAL4 of the CC V2.3 part 3 assurance requirements which is augmented with ADV_IMP.2, ALC_DVS.2 ATE_DPT.2, and AVA_VLA.4; thus, it is assigned the verdict 'pass' on the basis of the paragraph 175 of the CC V2.3 part 1. In addition, the TOE satisfies the Smart Card Open Platform Protection Profile for Government V1.0 (December 28, 2004)

MULTOS SM10 R2 (the TOE), developed by SAMSUNG SDS, is an operating system for the ICC(integrated circuit card) or smartcard, which is designed in order that multiple applications can be loaded and executed on the smartcard in a highly interoperable and secure manner.

The TOE of SAMSUNG SDS SM10 R2 is MULTOS which consists of MULTOS operating system ROM code and AMD(Additional MULTOS Data) loaded on S3CC9RB or S3CC9P9 smartcard controller. The TOE provides interoperable API(application programming interface), that enables applications to be executed independent of the underlying hardware layer.

On the other hand, the TOE is used in connection with IFD(Interface Device) or CAD(Card Acceptance Device) such as ATM(Automatic Teller Machine), ISO 7816 compliant POS(Point-of-Sale) terminal, or dummy card reader so that smartcard applications are loaded and executed on it.

MCD(MULTOS Carrier Device) sends ATR(Answer-to-Reset) to IFD whenever it receives reset signal from IFD. IFD sends commands to MCD and receives responses from MCD resulting in command-response communication.

The TOE consists of the following modules:

- MULTOS Functional Module – high level functionality being performed while communicating with IFD
- MULTOS Memory Manager – partition of EEPROM memory by functional block and change management of memory

- Secure Writing Module – controls to writing data onto EEPROM including atomicity
- Cryptographic Module – cryptographic functionality used in MEL(MULTOS Executable Language) applications
- Application Abstract Machine – separation of MEL applications

The security functions provides by the TOE are as follows:

- adequate integrity verification and authentication of each application when loaded onto or deleted from MULTOS-based smartcard
- Usage of a confidential application which is encrypted and meant to be decrypted in the course of application loading
- Protection of application from previously loaded applications or operating system dedicated area via separation of memory space and so forth
- adequate authentication of a MULTOS-based smartcard validated by MSM
- adequate authorization of defined features (e.g., strong cryptography) with regard to authorized applications
- Management of ratification count on defined principal functions (e.g., key installation, application loading, and application deletion)

The certification body has examined the evaluation activities and testing procedures of the evaluator; provided the guidance regarding the technical problems and evaluation procedures; reviewed each evaluation work package and the evaluation technical report. In this regard, the certification body has confirmed that the evaluation results assure the TOE meets all of the security function requirements and assurance requirements described in the ST. As a result, the certification body has certified that the observations and evaluation results made by the evaluator are accurate and reasonable; thus, certified that each verdict on each work package of the evaluator is correct.

Certification Validity: The information contained in the certification report means neither the use of SAMSUNG SDS MULTOS SM10 R2 is approved nor its qualification is assured by any Government Agency of the Republic of Korea.

2. TOE Identification

The [Table 1] describes the information about the TOE identification.

[Table 1] TOE identification

Evaluation Guidance	Korea IT Security Evaluation and Certification Guidance (2005. 5. 21) Korea IT Security Evaluation and Certification Scheme (2005. 9. 22)
TOE	SAMSUNG SDS MULTOS SM10 R2
Protection Profile	Smart Card Open Platform Protection Profile for Government V1.0 (2004. 12. 28)
Security Target	SM10 Security Target V1.2 (2006. 3. 15), SAMSUNG SDS
ETR	SAMSUNG SDS MULTOS SM10 R2 ETR, V 1.0 (2006. 8. 9)
Evaluation Result	Satisfies the Common Criteria V2.3 part 2 Satisfies the EAL 4 of the Common Criteria V2.3 part 3 assurance requirements augmented with ADV_IMP.2, ALC_DVS.2, ATE_DPT.2, and AVA_VLA.4
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation V2.3 (2005. 8)
Evaluation Methodology	Common Methodology for Informations Technology Security Evaluation V2.3 (2005. 8)
Sponsor	SAMSUNG SDS
Developer	SAMSUNG SDS
Evaluation Team	KISA IT Security Evaluation Center, Evaluation Team I Yeowoong Yoon, Seongjae Lee, Kyungho Son
Certification Body	National Intelligence Service

SAMSUNG SDS MULTOS SM10 R2 is a smartcard operating system masked onto ICC, and designed to be able to load and execute multiple applications in a highly interoperable and secure manner on smartcard

The underlying hardware specification is as stated in the [Table 2].

[Table 2] The underlying hardware specification of the TOE

CPU	16-bit CalmRISC 16 core
ROM	ROM : 160Kbytes(S3CC9P9), 320Kbytes(S3CC9RB) - User area : 144K bytes, 304K bytes - Crypto Library : 16K bytes
EEPROM	64Kbytes(S3CC9RB), 32Kbytes(S3CC9P9)
RAM	6K bytes
Crypto-Coprocessor	- Module exponential accelerator - SHA-1 accelerator
DES/3-DES	Built-in hardware DES/3-DES
Other H/W	- MPU(Memory Protection Unit) - 16bit RNG(Random Number Generator) - Timer : 16bit Timer and 20bit Watchdog Timer - Clock : 2.5MHz, 5MHz, 10MHz

3. Security Policy

The TOE operation conforms to the security policies stated below:

P.Separation of Duties The TOE should be securely managed according to separated responsibility from the smartcard manufacturing stage to usage.

P.Cryptography The cryptographic algorithms and modules only approved by National Intelligence Service should be used in the TOE.

P.Open Platform The TOE should be developed as an open platform where multiple applications can be loaded and executed.

4. TOE Assumptions and Scope

4.1 Assumptions

The TOE installation and operation should conform to the assumptions stated below.

A.Attacker Level	The attacker possesses a high level of expertise, resources, and motivation. Chances of the attacker finding an exploitable vulnerability are high.
A.Secure Channel	A secure communication channel exists between the TOE and the IFD.
A.Application	Installation of a new application onto the TOE is conducted in accordance with an authorized procedure, and the adequately installed application does not include any malicious code.
A.Hardward Layer	The underlying hardware of the TOE is physically secure.
A.TOE Management	In each stage from manufacturing to usage of the TOE, the roles are separated between manufacturers, issuers and cardholders, and responsibility of each is instructed adequately in accordance with prescribed rules. The TOE or smartcard is repaired or replaced in a secure manner in case of abnormal operations.
A.TSF Data	TSF data flowed out of the TOE are securely managed in the course of the TOE operation.

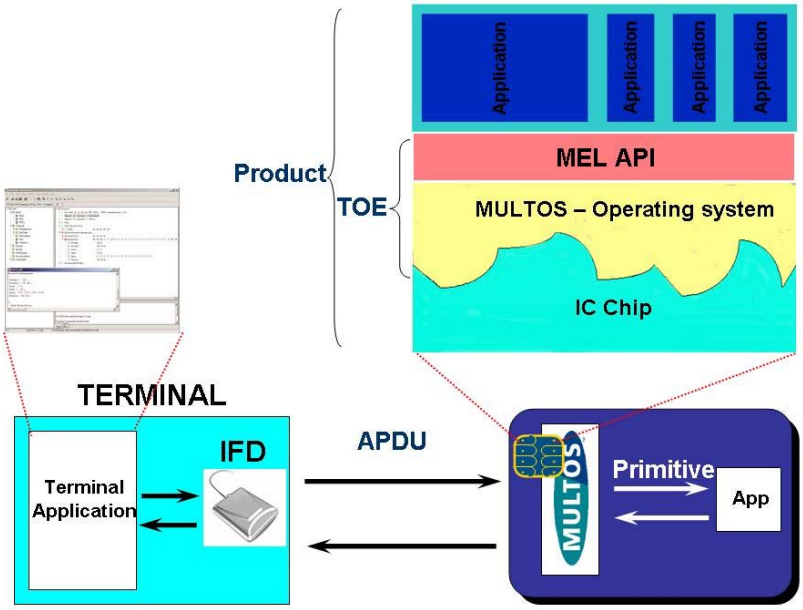
4.2 Scope to counter threats

The TOE provides a means to counter a security threat, such as attempts to infringe the TOE's own asset. In addition, the TOE provides a counter-measure for a direct physical attack that makes the SFP ineffective or bypasses, and provides a means to counter threat agents possessing high-level expertise, resources, and motivation as well.

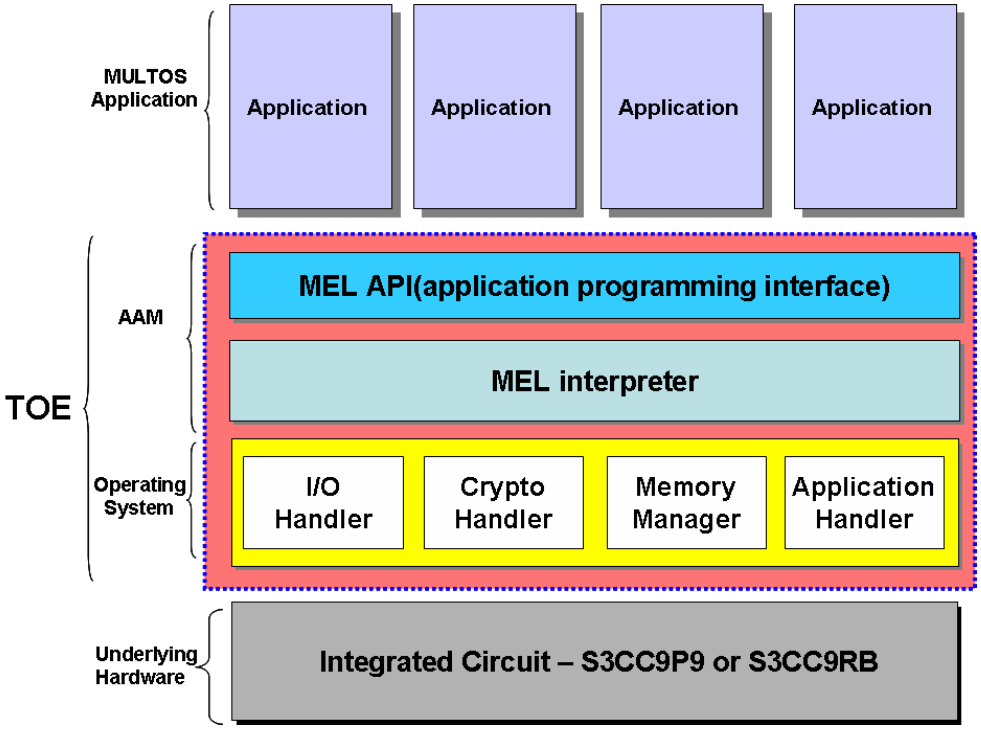
All security objectives and security policies are described to provide a means to counter an identified security threat.

5. TOE Information

The TOE provides security functions including secure application loading and the operational environment as showed in [Figure 1]. The simplified architecture of the TOE is as showed in [Figure 2].



[Figure 1] SAMSUNG SDS MULTOS SM10 R2 Operational Environment



[Figure 2] SAMSUNG SDS MULTOS SM10 R2 Simplified Architecture

The TOE consists of the following major subsystems.

- Application Abstract Machine Subsystem (SS_AM)

SS_AM performs MEL applications and MEL codelets in a secure manner. When an instruction or a primitive is requested to be executed by a MEL application, SS_AM checks whether the MEL application can execute it.

- Command Handler Subsystem (SS_CH)

SS_CH dispatches MULTOS commands and provides each command with interface through which commands are sent to other subsystems e.g., SS_MM. The commands in the protected mode such as Check Data, Set MSM Controls Data are processed and responded in SS_CH.

- Memory Management Subsystem (SS_MM)

SS_MM conducts memory management of MEL applications and MEL codelets. It is responsible for: opening, loading, creating new applications; entering and exiting applications; changing the currently selected codelet; providing access controls within currently active application and between two different applications.

- Cryptographic Function Subsystem (SS_CF)

SS_CF manages all the cryptographic operations required by MULTOS key management scheme and MEL applications with respect to MSM Controls data, creation of MEL applications and so forth. It supports authentication, signature generation/verification, encryption/decryption and random number generation.

6. Guidance

The TOE provides the following guidances:

- SAMSUNG SDS MULTOS SM10 R2 Administrator Guidance V1.5, Jun. 13, 2006
- SAMSUNG SDS MULTOS SM10 R2 User Guidance V1.5, Jun. 13. 2006
- SAMSUNG SDS MULTOS SM10 R2 Delivery and Operation Guidance V1.2, Jun. 22, 2006

7. TOE Test

7.1 Developer's test

- Test Method

The developer produced the test, considering the security function of the TOE. Each test is described in test documentation. Each test described in the test documentation includes the following items in detail:

- Testing No./Tester : The identifier of the test and the developer who participated in testing
- Purpose of the test : Description of the purpose of the test including security function of test subject and security module
- Test configuration : Detailed test configuration to carry out the testing
- Detailed test procedure : Detailed procedure to test security functions
- Expected result : The expected test result when implementing test procedure
- Actual result : The test result when implementing actual test procedure
- Comparison of the expected result and the actual result : The result of comparison of the expected result and the actual result

The evaluator evaluated the reasonability of the testing such as the test configuration, test procedure, analysis of test scope and the test of low-level design. The developer assured that the developer's test and test results are adequate for the evaluation configuration.

- Test configuration

The test configuration described in the test documentation includes the detailed configuration such as the test configuration, the TOE, the smartcard where the TOE is masked, or the probe board of the TOE. In addition, it describes detailed test configuration such as the test tools required for test.

- Test scope analysis/Low-level design test

The detailed evaluation results are described in the evaluation result in ATE_COV and ATE_DPT.

- Test Result

The test documentation describes the expected result and the actual result of each test. The actual result is confirmed through not only responses including APDU of the TOE but the audit record.

7.2 Evaluator's test

The evaluator configured the TOE by using the evaluation configuration and evaluation tools identical to the developer test, and examined the overall tests provided by the developer. The evaluator assured that the actual test result is consistent with the expected result.

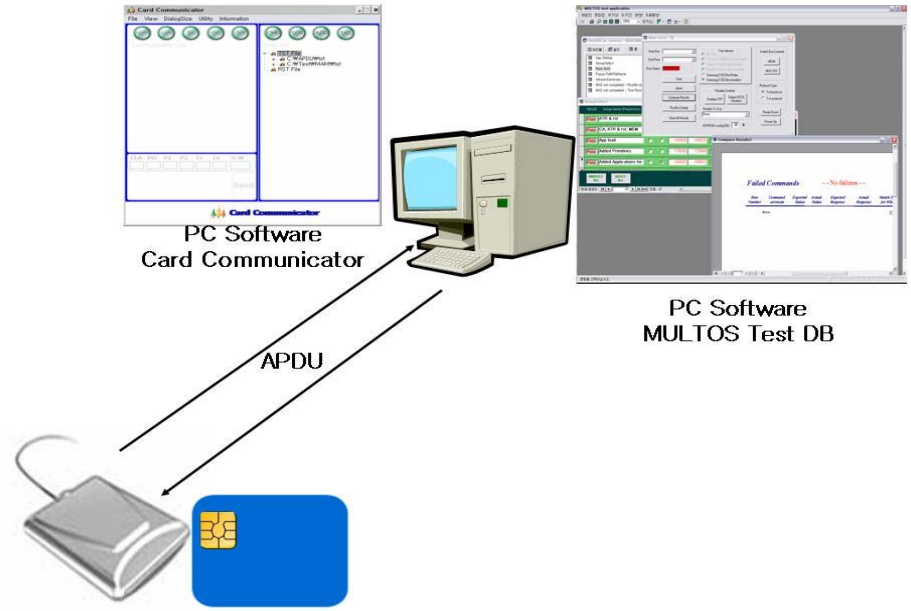
Moreover, the evaluator devised evaluator tests additionally on the basis of developer test, and confirmed that the actual test result is consistent with the expected test result.

The evaluator carried out the vulnerability test, and there is no vulnerability for malicious use in the evaluation configuration.

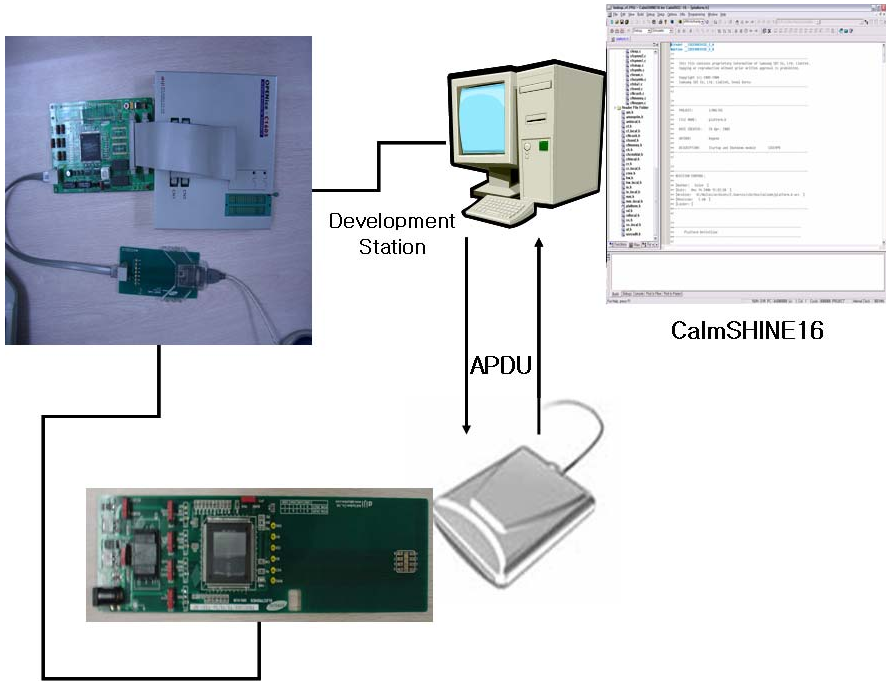
The evaluator's test result assured that the TOE works normally as described in the design documentation.

8. Evaluation Configuration

The evaluation configuration for the evaluator's test is conducted by the evaluator in a consistent manner with the developer's configuration described in the ST, which is shown in [Figure 3] and [Figure 4].



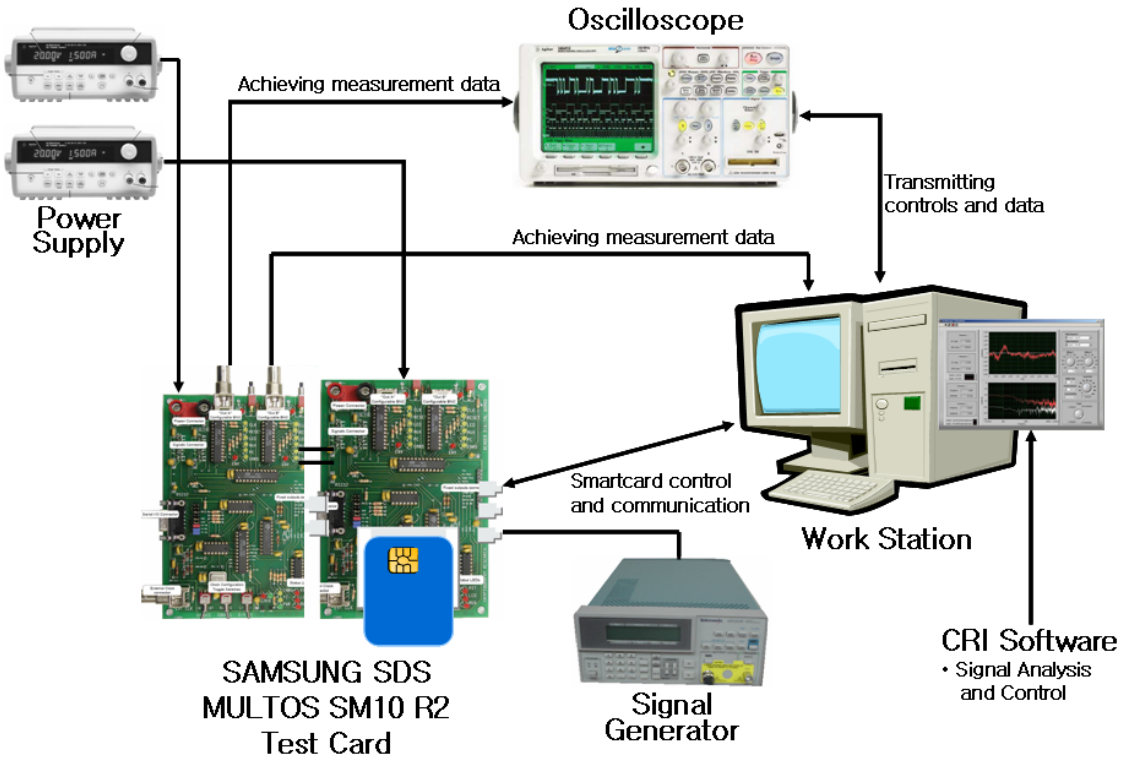
[Figure 3] TOE Evaluation Configuration (Functional testing using database)



[Figure 4] TOE Evaluation Configuration (Functional testing using debugging)

A smartcard or a probe board which carries the TOE is inserted to a CAD(Card Acceptance Device), with which test scripts stored in the MULTOS test database and those created by the evaluator are executed through a software, named Card Communicator in order to exchange APDUs.

The configuration of [Figure 5] is used for the penetration testing.



[Figure 5] Penetration testing Configuration

9. Evaluation Result

The evaluation is on the basis of the Common Criteria for Information Technology Security Evaluation and Common Methodology for Informations Technology Security Evaluation V2.3. It concludes that the TOE satisfies the CC V2.3 part 2 and EAL4 of the CC V2.3 part3 assurance requirements augmented with ADV_IMP.2, ALC_DVS.2, ATE_DPT.2, and AVA_VLA.4. The detail information regarding the evaluation is described in the ETR.

- ST evaluation (ASE)

The evaluator applied the ASE sub-activities described in the CC V2.3 to the evaluation of the ST of the TOE.

The ST introduction is complete and consistent with all the other parts of the ST, and correctly identifies the ST. The statement of TOE security environment in the ST provides a clear and consistent definition of the security problem that the TOE and its environment is intended to address. The security objectives are described completely and consistently, and they counter the identified threats, achieve the identified organizational security policies and are consistent with the stated assumptions. The TOE security requirements and the security requirements for the IT environment are described completely and consistently, and that they provide an adequate basis for development of a TOE that will achieve its security objectives. The TOE summary specification provides a clear and consistent high-level definition of the security functions and assurance measures, and that these satisfy the specified TOE security requirements. The ST is a correct demonstration of any PP for which compliance is being claimed.

Thus, the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding the TOE evaluation.

- Configuration Management Evaluation (ACM)

The evaluator applied the ACM sub-activities described in the CC V2.3 to the evaluation of the configuration management of the TOE.

From the configuration management documentation, it is confirmed that the developer has clearly identified the TOE and its associated configuration items, means to identify each configuration, means to assign versions, and means to control change of configuration items. From the configuration

management documentation, it is confirmed that configuration management system is applied to each implementation representation when developed and the developer controls changes to the implementation representation with the support of organizational configuration management personnel and system.

Thus, configuration management documentation assists the consumer in identifying the evaluated TOE and ensures that configuration items are uniquely identified, and the adequacy of the procedures that are used by the developer to control and track changes that are made to the TOE.

- Delivery and Operation Evaluation (ADO)

The evaluator applied the ADO sub-activities described in the CC V2.3 to the evaluation of the delivery and operation of the TOE.

The delivery and operation documentation describes all procedures and steps used to maintain security and detect modification or substitution of the TOE when distributing, installing, starting, and operating the TOE.

By inspection of all the sites relevant to the TOE, evaluator confirms that the delivery and operation documentation used is adequate to ensure that the TOE is distributed, installed, started, and operated in the same way the developer intended it to be and that it is delivered without modification.

- Development Evaluation (ADV)

The evaluator applied the ADV sub-activities described in the CC V2.3 to the evaluation of the development of the TOE.

The following design documentation is adequate to understand how the TSF provides the security functions of the TOE in each step; the functional specification which describes the external interfaces of the TOE, high-level design which describes the architecture of the TOE in terms of internal subsystems, low-level design which describes the architecture of the TOE in terms of internal modules, implementation representation of the source code level description, and the representation correspondence which maps representations of the TOE to one another in order to ensure consistency.

The representation correspondence shows the developer has correctly and completely implemented the requirements of the ST, the functional specification, the high-level design and the low-level design in the implementation representation.

- Guidance Evaluation (AGD)

The evaluator applied the AGD sub-activities described in the CC V2.3 to the evaluation of the guidance of the TOE.

The user guidance is adequate to demonstrate how to access and operate the TOE via user interface and the administrator guidance describes how to administer the TOE in a secure manner during administrative operation with instances and matters that require attention.

It is confirmed that user guidance and administrator guidance are correctly performed as specified.

- Life Cycle Support Evaluation (ALC)

The evaluator applied the ALC sub-activities described in the CC V2.3 to the evaluation of the life cycle support of the TOE.

It is confirmed that the procedures the developer uses during the development and maintenance of the TOE are adequately described in the life cycle support of the TOE; these procedures include the security measures used throughout TOE development, the life cycle model used by the developer, and the tools used by the developer, the scheme used by the developer throughout the life cycle of the TOE.

By inspection of the relevant sites, evaluator confirms that the life cycle support of the TOE used is applied as specified.

- Tests Evaluation (ATE)

The evaluator applied the ATE sub-activities described in the CC V2.3 to the evaluation of the test of the TOE.

The developer's test documentation describes and demonstrates test objectives, test steps and procedures, test results with expected results. By repeatedly testing functional tests of each development step provided, the evaluator confirmed that the TOE behaves as specified, and to gain confidence in the developer's test results by performing entire developer's tests.

By independently testing a subset of the TSF, it is confirmed that TSF behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST.

- Vulnerability Assessment Evaluation (AVA)

The evaluator applied the AVA sub-activities described in the CC V2.3 to the evaluation of the vulnerability assessment of the TOE.

The vulnerability analysis document describes adequately and accurately that appropriate measures are in place to prevent the exploitation of obvious vulnerabilities and possible misuses in the intended environment or indicates the guidance for that; the evaluator has conducted the independent vulnerability analysis to confirm the accuracy of the developer's vulnerability analysis document. From the strength analysis of security functions, it is addressed that the strength of TSF satisfies the requirement specified in PP/ST .

10. Recommendations

- The TOE is able to prevent failed security functions, such as loading or deleting applications, from being used when the number of failure exceeds a retry counter. The retry counter is meant to be specified by the administrator of the TOE and thus the specified value is recommended to be less than 10.
- The ADC(Application Delete Certificate) is used to delete an application. The AID(Application Identifier) should be assigned as a different value from one another when developed, since an identical AID of two different applications results in an identical ADC.
- The value of random seed, which is used to load an application as one of the MSM data, should be set to "non-zero" when applications are developed, since re-loading an application which has been deleted may be possible even without a permission of the MSM if only the value of random seed is "zero".

11. Abbreviations and Terms

The following abbreviations and terms are used in the certification report.

(1) Abbreviations

AID	Application Identifier
APDU	Application Protocol Data Unit
API	Application Programming Interface
ATM	Automated Teller Machine
ATR	Answer To Reset
CAD	Card Acceptance Device
CC	Common Criteria
CLA	Class
COS	Chip Operating System
CRT	Chinese Remainder Theorem
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read-Only Memory
EF	Elementary File
FID	File Identifier
IC	Integrated Circuit
IFD	Interface Device
PP	Protection Profile
RAM	Random-Access Memory
ROM	Read-Only Memory
RNG	Random Number Generator
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

(2) Terms

AAM (Application Abstract Machine)
Virtual machine. Applications are developed in accordance with the interface of it implemented onto the MULTOS operating system.

ADC (Application Delete Certificate)
An Application Delete Certificate contains permission for an application to be

deleted from one or more MULTOS cards. The certificate contains the AID of the application to be deleted. To delete an application the certificate is presented to a card. The card checks the certificate, and if valid, will delete the application.

AID (Application Identifier)
Unique identifiers of smartcard applications assigned in accordance with ISO 7816

ALC (Application Load Certificate)
An Application Load Certificate contains permission for an application to be loaded onto one or more MULTOS cards. Neither the Key Management Authority nor the Issuer needs to know the contents of the specific application for which they are providing the certificates. This allows the application provider to keep private the contents of the code and data being loaded.

ALU (Application Load Unit)
A unit which applications are loaded to MULTOS cards as. An application load unit consists of code and data.

Application (MEL Application)
MULTOS Executable Language and associated data

Application Developer
A person or a company who develops applications. Sometimes Application Developer is identical to Application Provider or ALU Provider.

Application Provider
A person or a company who provides applications or ALUs to issuers.

APDU (Application Protocol Data Unit)
Command-response set between a smartcard and a CAD which is defined in ISO 7816

COB (Chip On Board)
A module where a semiconductor chip is embedded on a plastic board, connected to gold-plated electrodes, and finalized with phenol resin.

Codelet
Contrary to the normal assumption that the whole of the application will be loaded into EEPROM at some stage, it is possible to save EEPROM space

that will be taken up by the code(which does not change) by moving sections of the code into ROM; this code is called a Codelet.

EEPROM(Electrically Erasable Programmable Read-Only Memory)
EEPROM is a special type of PROM that can be erased by exposing it to an electrical charge. Like other types of PROM, EEPROM retains its contents even when the power is turned off. Also like other types of ROM, EEPROM is not as fast as RAM. EEPROM is similar to flash memory (sometimes called flash EEPROM). The principal difference is that EEPROM requires data to be written or erased one byte at a time whereas flash memory allows data to be written or erased in blocks. This makes flash memory faster.

Emulation Board
A printed circuit board where specific programming technology or mechanism can be used for a computer system to imitate another system

ICC (Integrated Circuit Card)
A small electronic device about the size of a credit card that contains electronic memory consisting of mask ROM, EEPROM, and RAM, and possibly an embedded integrated circuit (IC) with CPU and I/O handler

IFD (Interface Device)
Data communication devices connecting ICC to external system

KMA (Key Management Authority)
The entity which provides digital certificates such as ALCs, ADCs and Enablement Data

KTU (Key Transformation Unit)
A Key Transformation Unit (KTU) is required when loading Confidential Application Load Units. The purpose of the KTU is to protect the keys used in making the ALU confidential. The KTU will normally be created as part of the data preparation / ALU generation process. During application loading the KTU is used by the card to decrypt the confidential ALU.

MCD (MULTOS Carrier Device)
ICC that carries MULTOS operating system

MSM (MULTOS Security Manager)
Key Management Authority. MSM controls security conditions of every MCD specified using msm-cd and enables MCD from protected mode.

MEL(MULTOS Executable Language)
The instruction set of the Application Abstract Machine, as defined in the MULTOS Developers Reference Manual

MISA(MULTOS Injection Security Application)
A secure application device distributed by KMA, which injects 64-byte security data to each MCD in a secure manner

MULTOS (Multi-application Operating System)
A name of operating system usually implemented on ICC to operate multiple application in a highly secure manner. It also implies the scheme of management and operation for the life cycle of MULTOS carrier device. MULTOS employs an end-to-end trust architecture that places the Issuer in control of their card base.

M-SPI (MULTOS Service Provider Interface)
A software tool which enables Issuers and Bureaux to request card enablement data and application load & delete certificates.

PIN (Personal Identification Number)
An identification number used to authenticate the card holder

RAM(Random Access Memory)
A type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes. There are two basic types of RAM: dynamic RAM (DRAM), static RAM (SRAM). The two types differ in the technology they use to hold data, dynamic RAM being the more common type. Dynamic RAM needs to be refreshed thousands of times per second. Static RAM does not need to be refreshed, which makes it faster; but it is also more expensive than dynamic RAM. Both types of RAM are volatile, meaning that they lose their contents when the power is turned off.

ROM(Read-Only Memory)
A computer memory on which data has been prerecorded. Once data has been written onto a ROM chip, it cannot be removed and can only be read. Unlike main memory (RAM), ROM retains its contents even when the computer is turned off. ROM is referred to as being nonvolatile, whereas RAM is volatile.

Virtual Machine
Virtual platform implemented onto operating system which provides application

programming interfaces independent of hardware platform(semiconductor for ICC)

12. Reference

The certification body has used the following documents to produce the certification report:

[1] Common Criteria for Information Technology Security Evaluation (May. 21, 2005)
[2] Common Methodology for Information Technology Security Evaluation V2.3
[3] Smart Card Open Platform Protection Profile for Governmenr V1.0 (Dec. 28, 2004)
[4] Korea IT Security Evaluation and Certification Guidance (May. 21, 2005)
[5] Korea IT Security Evaluation and Certification Scheme (Sep. 22, 2005)
[6] SAMSUNG SDS MULTOS SM10 R2 Security Target V1.2 (Mar. 15, 2006)
[7] SAMSUNG SDS MULTOS SM10 R2 Evaluation Technical Report V1.2 (Oct. 9, 2006)