KECS-CR-08-34

S3FS91J/S3FS91H/S3FS91V Certification Report

Certification No.: KECS-ISIS-0117-2008

SEP. 2008

National Intelligence Service

IT Security Certification Center

This document is the certification report on smartcard chip S3FS91J/S3FS91H/S3FS91V of Samsung Electronics. Co. Ltd.

Certification Committee Members

I. J. Yun (ETRI)
S. D. Cha (Korea university)
D. S. Seo (Sunshin wemen's university)
H. J. Lee (Dongseo university)
J. C. Ha (Hoseo university)

Certification Body

IT Security Certification Center, National Intelligence Service

Evaluation Facility

Korea Information Security Agency.

Table of Contents

1. Overview

This report describes the certification result drawn by the certification body on the results of the EAL4+ evaluation of S3FS91J/S3FS91H/S3FS91V with reference to the Common Criteria for Information Technology Security Evaluation (notified May.21, 2005, "CC" hereinafter). It describes the evaluation result and its soundness and confirmity.

The evaluation of the TOE has been carried out by Korea Information Security Agency and completed on 29. August 2008. This report grounds on the evaluation technical report (ETR) KISA had submitted, in which the evaluation has confirmed that the product had satisfied the CC Part 2 and EAL4+ of the CC Part 3 and had been "suitable" according to the CC Part 1, paragraph 191.

Developed by Samsung Electronics Corp. and sponsored by Samsung Electronics. Co., Ltd, S3FS91J/S3FS91H/S3FS91V designed and packaged specifically for Smart Card applications. The products maintain the integrity and the confidentiality of content of the smartcard memory as required by the application and maintain the correct execution of the software are residing on the card.

The CB has examined the evaluation activities and test procedures, provided the guidance for the technical problems and evaluation procedures, and reviewed each evaluation work package report and evaluation technical report. Consequently, the CB has confirmed that the evaluation results had ensured that the TOE had satisfied all security functional requirements and assurance requirements specified in the ST, thus the observations and evaluation results made by the evaluator had been correct and reasonable, and the verdicts assigned by the evaluator on the product had been correct.

Certification validity: The Information in this certification report does not mean the the use of this product is approved or that its quality is guaranteed by the government of Republic of Korea.

2. TOE Identification

[Table 1] identifies the TOE.

[Table 1] TOE identification

Evaluation guidance	Korea IT Security Evaluation and Certification Guidance (Notification No.2007-31 by the MIC, Aug. 22, 2007) Korea IT Security Evaluation and Certification Scheme (NIS, Dec. 1, 2007)
TOE	S3FS91J/S3FS91H/S3FS91V
Protection profile	Smartcard IC platform protection profile BSI-PP-002 V11.0
Security target	Security Target of S3FS91J/S3FS91H/S3FS91V V32-bits RISC Microcontroller For Smart Card V1.5(2008.8.27)
ETR	S3FS91J/S3FS91H/S3FS91V Evaluation Technical Report V1.00 (Aug. 25, 2008)
Evaluation result	Satisfies CC Part 2 Satisfies CC Part 3
Evaluation criteria	Common criteria for information technology security evaluation V2.3 (Notification No.2005-25 by the MIC, 21 May 2005)
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation V2.3 (Aug. 2005)
Sponsor	Samsung Electronics. Co., Ltd
Developer	Samsung Electronics. Co., Ltd
Evaluator	Kyumin Cho, Sungjae Lee, Kyoungho Son Korea Information Security Agency
Certification body	National Intelligence Service

The TOE designed and packaged specifically for Smart Card applications. The products maintain the integrity and the confidentiality of content of the smartcard memory as required by the application and maintain the correct execution of the software are residing on the card. In the [Table 2] shows system configuration of the TOE

[Table 2]

CPU	- 32-bits SC100 RISC processor - Memory Protection Unit(MPU) 포함
ROM	- 32K bytes ROM / 8K bytes TEST ROM - Secure Bootloader
RAM	- 20K bytes RAM (2K bytes는 Crypto로 사용)
Flash Memory	- 768K bytes(S3FS91J) / 512K bytes(S3FS91H) / 420K bytes(S3FS91V)
3DES	- Built-in hardware Triple DES (3DES) accelerator
Crypto Accelerator	- Secure TORNADO™ cryptographic coprocessor’s modular multiplier RSA cryptography (1024 ~2048 bits)
기타	- Detector & Security Controller : High and Low Temperature detectors, High and Low Frequency detectors, High and Low Supply Voltage detectors, Supply Voltage Glitch detectors, Light detector, Active Shield against physical intrusive attacks, Dynamic data bus encryption - Internal Voltage Regulator(IVR) - Interrupts Controller - Serial I/O Interface : UART, ISO7816 - Power-on Reset - Random Number Generator - CRC : Hardware parity/CRC calculator - Timers - Clock controller - Bus : AMBA bus

3. Security Policy

The TOE must apply the security polices as specified below

P.Process-TOE	The TOE must ensure that the development and production of the Smartcard Integrated Circuit is secure so that no information is unintentionally made available for the operational phase of the TOE. For example, the confidentiality and integrity of design information and test data shall be guaranteed; access to samples, development tools and other material shall be restricted to authorized persons only; scrap will be destroyed etc.
P.Add-Functions	The TOE shall provide the following specific security functionality to the Smartcard Embedded Software: • Triple Data Encryption Standard (Triple DES (3DES)) • Rivest-Shamir-Adleman (RSA) public key asymmetric cryptography • Hardware parity/CRC calculator

4. Assumptions and Scope

4.1 Assumptions

The TOE shall be installed and operated with the following assumptions in consideration:

A.Process-Card	TOE가 end-user에게 전달된 이후(packaging, finishing, personalization 단계)에도 TOE의 제조 및 test data에 대한 무결성과 비밀성이 유지되어야 한다.
A.Plat-Appl	TOE Hardware Platform을 사용하는 Smartcard Embedded software는 TOE가 배포하는 문서들의 요구사항에 맞도록 설계되어야 한다.
A.Resp-Appl	Smartcard Embedded Software에서는 모든 사용자 데이터를 관리한다.
A.Key-Function	키 사용과 관련된 기능은 Smartcard Embedded Software에 구현되어 있어야 한다.
A.Key-Management	RSA키를 생성하고 관리하는 기능이 Smartcard Embedded Software에 있어야 하며, TOE가 배포하는 문서들의 요구사항에 맞도록 설계되어야 한다.
A.Multi-Appl	Multi application 환경에서 application 간에 memory access control 기능이 Smartcard Embedded Software에 필요하다.
A.EncData-Appl	Multi application 환경에서 application 간에 data 암호화기능이 Smartcard Embedded Software에 필요하다.
A.Leak-Crypto	Smartcard Embedded Software에서 TOE의 누수 공격에 대한 방어 기능을 사용할 때 TOE가 배포하는 문서들의 요구사항에 부합되어야 한다.

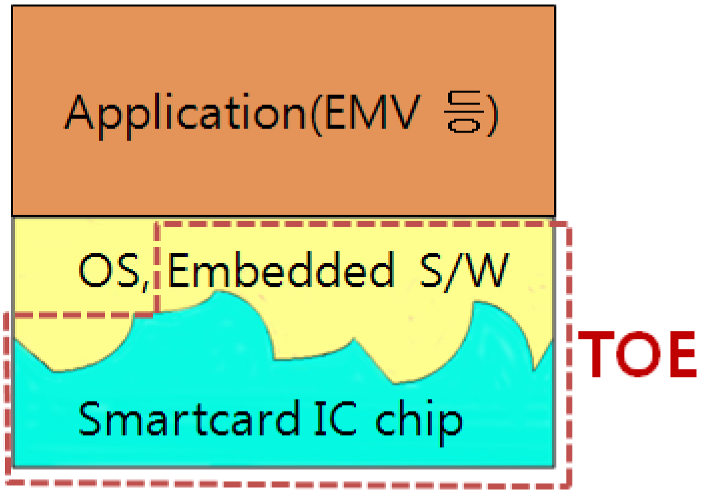
4.2 Scope to Counter a Threat

The TOE provides a means appropriate for the IT environment of the TOE to counter a security threat but not a means to counter a direct physical attack that causes malfunction of the TOE. The TOE also provides a means to take actions on any logical attacks launched by a threat agent possessing low-level expertise, resources, and motivation in the networks of the TOE.

All security objectives and security policies are described such that a means to counter identified security threats can be provided.

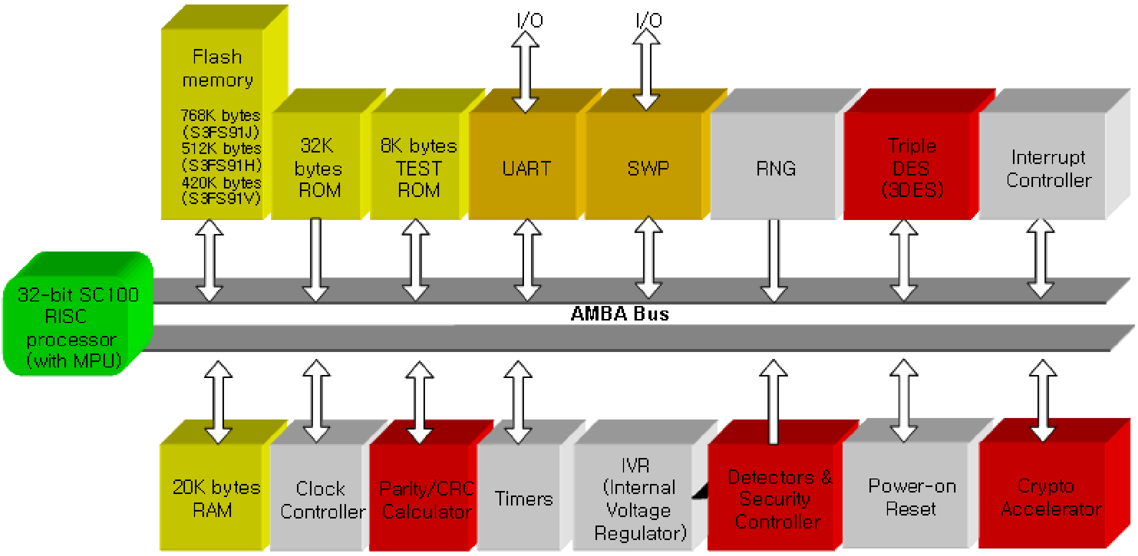
5. TOE Information

The TOE designed and provided security function for Smartcard Embedded Software. In the [Figure 1], shows the relationship between TOE and Embedded Software which is not part of the TOE.



[Figure 1] Relationship between TOE and Embedded Software

The TOE component is shows in [Figure 2]. And all components are sub system to provide security function for Smartcard Embedded Software.



[Figure 2] TOE components

The main security functions of the TOE are:

- Environmental Security violation recording and reaction

– The detectors and filters are use for preventing security violation.

- Access Control

– The TOE detects invalid address access occurrence on memory/flash.

- Non-reversibility of TEST and USER modes

– There is no way to return the TEST mode after selects the USER mode.

- Hardware countermeasures for unobservability

– This security function enforces hardware counter measures to enhance unobservability and it protects memory and address/data bus from probing attacks.

- Cryptography

– The TOE support Triple DES (3DES) and RSA algorithm and providesa mechanism to generate random numbers

6. Guidance

The TOE provides the following guidance documents.

– S3FS91J/1H/1V Administrator Guidance V1.1, Aug. 25, 2008

7. TOE Test

7.1 Developer's Test

- Developer's testing is detailed in the test documents.

The next table decribes the summary of developer test efforts required in the ATE_FUN.1-12 work unit evaluator's activity.

TOE Test Configuration	TOE for test	S3FS91J/1H/1V
	Test Setup 1	o IMS Equipment Logic Master XL-60 (v4.9)
	Test Setup 2	o ADVANTEST VLSI TEST SYSTEM T3326A, T3347 o TEMPTRONIC X-Stream 2000
	Test Setup 3	o Logic Simulator Sim Vision 05.10 – S012 o Analog Simulator Verilog
	Test Setup 4	o Oscilloscope o Power Supply o Pulse Generator o Probe Station Micromanipulator Model 7000-LTE o TEMPTRONIC Thermostream TP04010A o Micropross Card Reader Star 265 o PC with Windows2000 o Software Smart Card Evaluator for Samsung IC (SCESI) V2.2.0.2
	Test Setup 5	o Realview ice and Development system o PBS3FS91J Adapterboard for chip o PC with Windows XP o Software Smart Card Evaluator for Samsung IC (SCESI) V2.2.0.2

o Test results

The test document describes expected result and actual result of each test. The actual results can be confirmed both on the screen of the TOE and by audit records.

7.2 Evaluator's Test

The evaluator has installed the product using the same evaluation configuration and tools as the developer's test and performed all tests provided by the developer. The evaluator has confirmed that, for all tests, the expected results had been consistent with the actual results.

The evaluator has confirmed this consistency by performing additional tests based on the developer's test.

The evaluator has also confirmed that, after performing vulnerability test, no vulnerability had been exploitable in the evaluation configuration.

The evaluator's test result has ensured that the product had normally operated as described in the design documents.

8. Evaluation result

The evaluation is performed with reference to the CC V2.3 and CEM V2.3. The result claims that the evaluated product satisfies the requirements from the CC Part 2 and EAL4 in the CC Part 3. Refer to the evaluation technical report for more details.

1) Security Target evaluation (ASE)

The ST introduction is complete and consistent with all other parts of the ST and gives a correct identification of the ST.

The TOE description describes the objectives and functionality of the TOE sufficiently to be understandable and is coherent, complete, internally consistent, and consistent with all other parts of the ST.

The TOE security environment provides a clear and consistent definition of the security problems that are induced in the TOE and its environment in terms of assumptions, threats, and OSP(organizational security policy)s.

The security objectives are categorized into those for the TOE and those for the environment. They counter the identified threats, achieve the identified OSPs, and are consistent with the identified assumptions.

The IT security requirements describe the security functional and assurance requirements completely and consistently, and provide an adequate basis for development of a TOE that will achieve its security objectives.

TOE summary specification defines correctly and consistently the security functions and assurance measures that satisfy the described TOE security functional requirements.

The PP claims correctly identify the PP to which the ST claims conformance and ensure that the operations uncompleted in the PP are completed in the ST.

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

2) Configuration management evaluation (ACM)

The configuration management documentation describes that the changes to the implementation representation are controlled with the support of automated tools. It also clearly identifies the TOE and its associated configuration items and describes that the ability to modify these items is properly controlled.

The evaluator has confirmed by the CM documentation that the developer had performed configuration management on the TOE implementation representation, evaluation evidence required by the assurance components in the ST, and security flaws.

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

3) Delivery and operation evaluation (ADO)

The delivery documentation describes all procedures used to maintain security and detect modification or substitution of the TOE when distributing the TOE to the user's site.

The evaluator has confirmed that the procedures and steps for the secure installation, generation, and start-up of the TOE had been documented and resulted in a secure configuration.

Therefore, the delivery and operation documentation is adequate to ensure that the TOE is installed, generated, and started in the same way the developer intended it to be and that it is delivered without modification.

4) Development evaluation (ADV)

The functional specification adequately describes all security functions of the TOE and that the functions are sufficient to satisfy the security functional requirements of the ST. It also adequately describes the external interfaces to the TOE.

The high-level design describes the TSF in terms of subsystems, describes the interfaces to the subsystems, and correctly realizes the functional specification.

The low-level design describes the internal operation of the TSF in terms of internal modules. It describes the interrelationships and dependencies between the modules. It is sufficient to satisfy the functional requirements of the ST, and is a correct and effective refinement of the high-level design.

The implementation representation is sufficient to satisfy the functional requirements of the ST and is a correct realization of the low-level design.

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

The security policy model clearly and consistently describes the rules and characteristics of the security policies and describes their correspondence to the security functions in the functional specification and the security functional requirements in the ST.

Therefore, the development documentation is determined adequate to understand how the TSF provides the security functions of the TOE, as it consists of a functional specification (which describes the external interfaces of the TOE), a high-level design (which describes the architecture of the TOE in terms of internal subsystems), a low-level design (which describes the architecture of the TOE in terms of internal modules), an implementation description (a source code level description), a representation correspondence (which maps representations of the TOE to one another in order to ensure consistency), and a security policy model (which describes the rules and characteristics of the security policies enforced by the TOE).

5) Guidance documents evaluation (AGD)

The administrator guidance describes how the TOE is securely administered by the administrator. Therefore, it gives a suitable description of how to administer the TOE.

6) Life cycle support evaluation (ALC)

The evaluator has confirmed:

the developer's control of the development environment had been suitable to provide the confidentiality and integrity of the TOE design and implementation required for the secure operation of the TOE;

the developer had used a documented life-cycle model; and

the developer had used well-defined development tools with which one can get consistent and predictable results.

Therefore, the life-cycle support provides an adequate description of the security procedures and tools used in the whole development process and the procedures of the development and maintenance of the TOE.

7) Tests evaluation (ATE)

The tests have been sufficient to establish that the TSF had been systematically tested against the functional specification.

The evaluator has confirmed that the developer had tested the security functions of the TOE and the developer's test documents had been sufficient to show the security functions had behaved as specified.

The evaluator has determined, by independently testing a subset of the TSF, that the TOE had behaved as specified and gained confidence in the test results by performing all of the developer's tests.

Therefore, the tests have proved that the TSF had satisfied the TOE security functional requirements specified in the ST and behaved as specified in the functional specification and design documentation.

8) Vulnerability assessment evaluation (AVA)

The misuse analysis has confirmed that the guidance documentation had not been misleading, unreasonable, and conflicting, that secure procedures for all modes of operation had been addressed, and that the use of the guidance documentation had allowed insecure states of the TOE to be prevented and detected.

The evaluator has confirmed that the strength of TOE security function had been claimed for all probabilistic and permutational mechanism in the ST and the developer's SOF analysis had been correct.

The vulnerability analysis adequately describes the obvious security vulnerabilities of the TOE and the countermeasures such as the functions implemented or recommended configuration specified in the guidance documentation. The evaluator has confirmed by performing penetration testing based on the evaluator's independent vulnerability analysis that the developer's analysis had been correct.

The evaluator has determined by performing vulnerability analysis that there had not been any vulnerabilities exploitable by an attacker possessing a low attack potential in the intended TOE environment.

Therefore, based on the developer and evaluator's vulnerability analysis and the evaluator's penetration testing, the evaluator has confirmed that there had been no flaws or vulnerabilities exploitable in the intended environment for the TOE.

9. Recommendations

- The operational documents contain necessary information about the usage of the TOE and all security hints therein have to be considered.
- The TOE is delivered to Card Manufacturer and the Smartcard Embedded Software Developer. The actual end user obtains the TOE from the operating system producer together with the application which runs on the TOE.
- The Smartcard Embedded Software Developer receives all necessary recommendations and hit to develop his software in form of the delivered documentation.
- Application of the security advises given in [7] especially the recommendations for secure usage in [7, chapter 4].

10. Acronyms and Glossary

The following acronyms and glossary are used in this report:

(1) Acronyms

CC	Common Criteria
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
PP	Protection Profile
SF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

11. Reference

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

[1] Common Criteria for Information Technology Security Evaluation (21 May 2005)

[2] Common Methodology for Information Technology Security Evaluation V2.3 (Aug. 2005)

[3] Korea IT Security Evaluation and Certification Guidance (21 May 2005)

[4] Korea IT Security Evaluation and Certification Scheme (1 Dec. 2007)

[5] S3FS91J/1H/1V Security Target V1.5 (Aug.27, 2008)

[6] S3FS91J/1H/1V Evaluation Technical Report, V1.0 (Aug.25, 2008)

[7] Security Application Note, S3FS91J/S3FS91H/S3FS91V, V1.0 (Aug 27 2008)