PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2008/17

S3FS9CI 32-bit RISC microcontroller for S-SIM

Paris, 23rd of June 2008

Courtesy Translation

Warning

This report is designed to provide sponsors with a document enabling them to assess the security level of a product under the conditions of use and operation defined in this report for the evaluated version. It is also designed to provide the potential purchaser of the product with the conditions under which he may operate or use the product so as to meet the conditions of use for which the product has been evaluated and certified; that is why this certification report must be read alongside the evaluated user and administration guidance, as well as with the product security target, which presents threats, environmental assumptions and the supposed conditions of use so that the user can judge for himself whether the product meets his needs in terms of security objectives.
Certification does not, however, constitute a recommendation product from DCSSI (Central Directorate for Information Systems Security), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

Any correspondence about this report has to be addressed to:

Secrétariat Général de la Défense Nationale
Direction Centrale de la Sécurité des Systèmes d'Information
Centre de certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP
France

certification.dcssi@sgdn.gouv.fr

Reproduction of this document without any change or cut is authorised.

Certification report reference

DCSSI-2008/17

Product name

S3FS9CI 32-bit RISC microcontroller for S-SIM

Product reference

IC platform reference: S3FS9CI version 2

Software libraries reference: Test Rom code version 1, Secure Cryptographic library version 3.8S, RNG1 library version 3.0

Protection profile conformity

BSI-PP-0002-2001

Smart card IC Platform Protection Profile Version 1.0 July 2001

Evaluation criteria and version

Common Criteria version 2.3

compliant with ISO 15408:2005

Evaluation level

EAL 4 augmented

ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4

Developer

Samsung Electronics Co. Ltd

San#24 Nongseo-Ri, Giheung-Eup, Yongin-City, Gyeonggi-Do, 449-711, Korea

Sponsor

Samsung Electronics Co. Ltd

San#24 Nongseo-Ri, Giheung-Eup, Yongin-City, Gyeonggi-Do, 449-711, Korea

Evaluation facility

CEA - LETI

17 rue des martyrs, 38054 Grenoble Cedex 9, France
Phone: +33 (0)4 38 78 40 87, email : cesti.leti@cea.fr

Recognition arrangements

CCRA

SOG-IS

IT Security Certified

The product is recognised at EAL4 level.

Introduction

The Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated April, 18th 2002, and published in the "Journal Officiel de la République Française". This decree stipulates that:

- The central information system security department draws up **certification reports**. These reports indicate the features of the proposed security targets. They may include any warnings that the authors feel the need to mention for security reasons. They may or may not be transmitted to third parties or made public, as the principals desire (article 7).
- The **certificates** issued by the Prime Minister certify that the copies of the products or systems submitted for evaluation fulfil the specified security features. They also certify that the evaluations have been carried out in compliance with applicable rules and standards, with the required degrees of skill and impartiality (article 8).

The procedures are available on the Internet site www.ssi.gouv.fr.

Content

1. The product

1.1. Presentation of the product

The evaluated product is the S3FS9CI 32-bit RISC microcontroller developed by Samsung Electronics Co. Ltd.

The microcontroller aims to host one or several software S-SIM applications and can be embedded in a plastic support to create a Smartcard with multiple possible usages (secure identity documents, banking, health card, pay-TV or transport applications…) depending on the Embedded Software applications. The software applications are not in the scope of this evaluation.

1.2. Evaluated product description

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operation environment.
The security target is based on [PP0002].

1.2.1. Product identification

The configuration list [CONF §2] identifies the product's constituent elements.
The certified version of the product can be identified by the following elements:

- IC platform reference: S3FS9CI version 2;
- Software libraries references: "Test ROM Code" version 1.0, "Secure Crypto. Library" version 3.8S and "RNG1 Library" version 3.0.

The product is physically marked by identification code on the top metal layer. The flash memory is also written with all identification information. These identification data are detailed in configuration management document (cf. [CONF §2.2.2.2]).

1.2.2. Security services

The product provides mainly the following security services:

- Environmental Security violation recording and reaction;
- Access Control;
- Non-reversibility of TEST and USER modes;
- Hardware countermeasures for unobservability.

1.2.3. Architecture

The S3FS9CI product is made up of:

- A Hardware part:
  - A 16/32-bit SC100 RISC processor;
  - Memories: NOR Flash (768KB), ROM for the test program (8KB), ROM for the embedded applications (32KB), SRAM (50KB), Crypto RAM (2KB);

- Security Modules: memory protection unit, logic for memory encryption/decryption, on-the-fly integrity checking (CRC), security sensors (voltage, frequency and temperature);
- Functional Modules: I/O management in contact mode serial port, ISO7816 interface and an ISO7816 controller, DES/T-DES secure co-processing units, secure Tornado™ coprocessor for RSA Asymmetric Cryptographic Support.

- A dedicated software is embedded in ROM which comprises:
  - A modular arithmetic library v.3.8S for RSA Asymmetric Cryptography support (optional);
  - A library for the deterministic random number generator (DRNG);
  - IC dedicated software (tests).

1.2.4. Life cycle

The product’s life cycle is organised as follow:

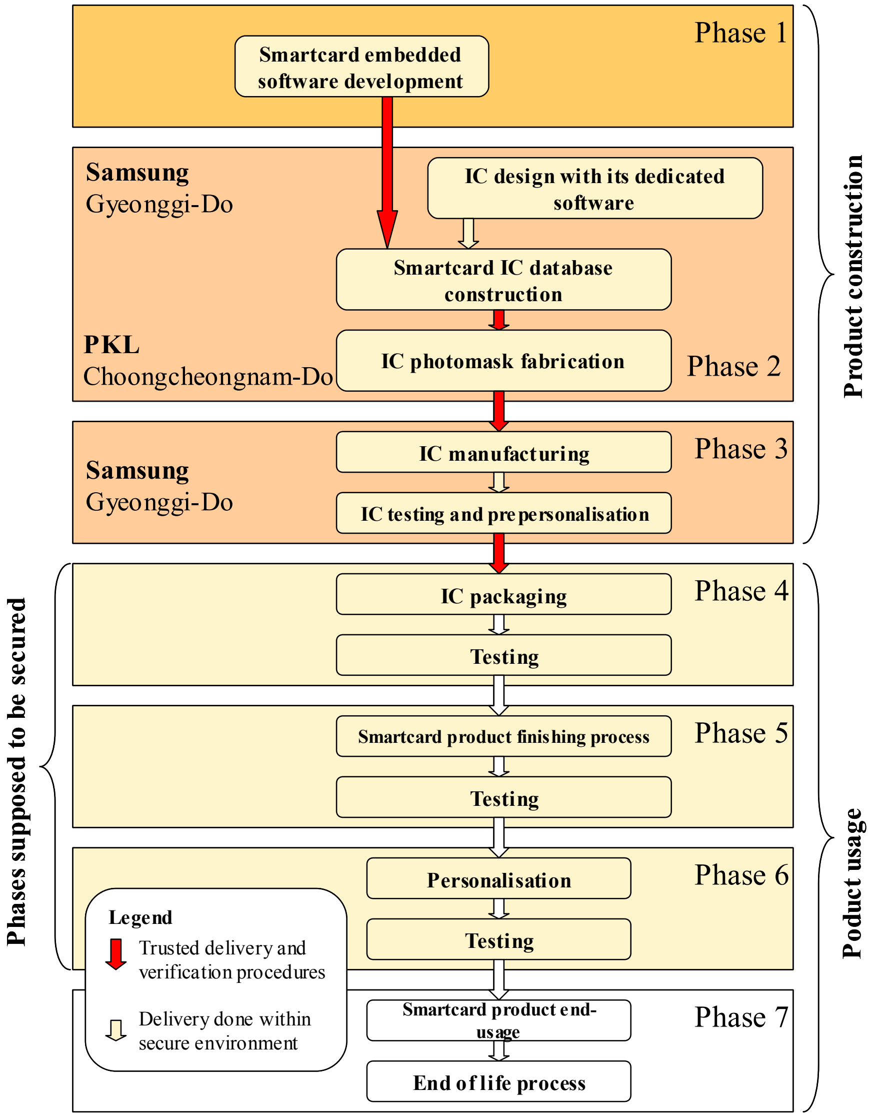
Phase 1
Smartcard embedded software development
Samsung
Gyeonggi-Do
IC design with its dedicated software
Smartcard IC database construction
PKL
Choongcheongnam-Do
IC photomask fabrication
Phase 2
Product construction
Samsung
Gyeonggi-Do
IC manufacturing
Phase 3
IC testing and prepersonalisation
IC packaging
Phase 4
Testing
Smartcard product finishing process
Phase 5
Testing
Personalisation
Phase 6
Testing
Phases supposed to be secured
Poduct usage
Legend
Trusted delivery and verification procedures
Delivery done within secure environment
Smartcard product end-usage
Phase 7
End of life process

Figure 1 – Life cycle

The product is designed by:

Samsung Electronics Co. Ltd - C&M Development team

San#24 Nongseo-Ri, Giheung-Eup,
Yongin-City, Gyeonggi-Do, 449-711,
Korea

The photo masks of the product are manufactured by:

PKL

493-3 Sungsung-dong, Cheonan-City,
Choongcheongnam-Do, 330-300,
Korea

The product is manufactured and tested by:

Samsung Electronics Co. Ltd – Line 5

San#24 Nongseo-Ri, Giheung-Eup,
Yongin-City, Gyeonggi-Do, 449-711,
Korea

The product is manufactured and tested by:

Samsung Electronics Co. Ltd – Line 2

San#24 Nongseo-Ri, Giheung-Eup,
Yongin-City, Gyeonggi-Do, 449-711,
Korea

The product can be in one of its three possible modes:

- "Test" mode: the product is tested using test features that are used at the end of the IC manufacturing within the secure developer premises. The TOE configuration is changed to "user" before delivery to the customer, and the part cannot be reversed to the "test" configuration;
- "User" mode: mode, in which the microcontroller runs under control of the smartcard embedded software. It is intended that customers and end-users will always use the microcontroller in user mode.

1.2.5. Evaluated configuration

This certification report applies to the microcontroller only. Any other software used for the evaluation is not part of the scope of certification.

The external large memory interfaces NAND (SLC and MLC) and OneNAND are not in the scope of the evaluation. The USB and MMC interface are also not in the scope of the evaluation.

With regard to the life-cycle, the evaluated product is the one at the end of its manufacturing phase (phase 3).

For the evaluation needs, the product S3FS9CI was provided to the ITSEF with a dedicated test embedded software, in a mode known as "open[1]".

[1] mode that enables to load and execute a native code in Flash and also to disable the configurable security mechanisms

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 2.3** [CC] and with the Common Evaluation Methodology [CEM].
For assurance components above EAL4 level, the evaluation facility own evaluation methods consistent with [AIS 34], validated by DCSSI have been used.

In order to meet the specificities of smart cards, the [CC IC] and [CC AP] guides have been applied.

2.2. Evaluation work

The evaluation relies on the evaluation results[1] of the S3CC9GW product certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) the 21st of February under the reference BSI-DSZ-CC-0400-2007.

The evaluation technical report [ETR], delivered to DCSSI the 18th of June 2008, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are "**pass**".

2.3. Cryptographic mechanisms robustness analysis

The robustness of cryptographic mechanisms has not been analysed by DCSSI.

2.4. Random number generator analysis

The evaluated product provides a deterministic random number generator that can be used by the embedded software. The evaluation facility has assessed along with DCSSI its conformance with the French standard for cryptography (cf. [REF-CRY]).

The deterministic generator reaches the "standard" level according to the French standard for cryptography (cf. [REF-CRY]*)*.

[1] Reuse of the results related to the development environment.

3. Certification

3.1. Conclusion

The evaluation was carried out according to the current rules and standards, with the required competency and impartiality for a licensed evaluation facility. All the work performed permits the release of a certificate in conformance with the decree 2002-535.

This certificate testifies that the product “S3FS9CI 32-bit RISC microcontroller for S-SIM” submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 4 augmented.

3.2. Restrictions

This certificate only applies on the product specified in chapter 1.2 of this certification report.

This certificate provides a resistance assessment of the S3FS9CI product to a set of attacks which remains generic due to the missing of any specific embedded application. Therefore, the security of a final product based on the evaluated microcontroller would only be assessed through the final product evaluation, which could be performed on the basis of the current evaluation results.

The user of the certified product shall respect the operational environmental security objectives summarized specified in the security target [ST] chapter 4.2 and shall respect the recommendations in the guidance [GUIDES].

3.3. Recognition of the certificate

3.3.1. European recognition (SOG-IS)

This certificate is issued in accordance with the provisions of the SOG-IS agreement [SOG-IS].

The European Recognition Agreement made by SOG-IS in 1999 allows recognition from Signatory States of the agreement[1], of ITSEC and Common Criteria certificates. The European recognition is applicable up to ITSEC E6 and CC EAL7 levels. The certificates that are recognized in the agreement scope are released with the following marking:

IT
Security
Certified

[1] The signatory countries of the SOG-IS agreement are: Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and United Kingdom.

3.3.2. International common criteria recognition (CCRA)

This certificate is released in accordance with the provisions of the CCRA [CC RA].

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries[1], of the Common Criteria certificates. The mutual recognition is applicable up to the assurance components of CC EAL4 level and also to ALC_FLR family. The certificates that are recognized in the agreement scope are released with the following marking:

[1] The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, the Republic of Korea, Malaysia, Netherlands, New-Zealand, Norway, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States of America.

Annex 1. Evaluation level of the product

Class	Family	Components by assurance level							Assurance level of the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Name of the component
ACM Configuration management	ACM_AUT				1	1	2	2	1	Partial CM automation
	ACM_CAP	1	2	3	4	4	5	5	4	Configuration support and acceptance procedures
	ACM_SCP			1	2	3	3	3	2	Problem tracking CM coverage
ADO Delivery and operation	ADO_DEL		1	1	2	2	2	3	2	Detection of modification
	ADO_IGS	1	1	1	1	1	1	1	1	Installation, generation and start-up procedures
ADV Development	ADV_FSP	1	1	1	2	3	3	4	2	Fully defined external interfaces
	ADV_HLD		1	2	2	3	4	5	2	Security enforcing high-level design
	ADV_IMP				1	2	3	3	2	Implementation of the TSF
	ADV_INT					1	2	3		
	ADV_LLD				1	1	2	2	1	Descriptive low-level design
	ADV_RCR	1	1	1	1	2	2	3	1	Informal correspondence demonstration
	ADV_SPM				1	3	3	3	1	Informal TOE security policy model
AGD Guidance	AGD_ADM	1	1	1	1	1	1	1	1	Administrator guidance
	AGD_USR	1	1	1	1	1	1	1	1	User guidance
ALC Life-cycle support	ALC_DVS			1	1	1	2	2	2	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD				1	2	2	3	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	Well-defined development tools
ATE Tests	ATE_COV		1	2	2	2	3	3	2	Analysis of coverage
	ATE_DPT			1	1	2	2	3	1	Testing: high-level design
	ATE_FUN		1	1	1	1	2	2	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	Independent testing – sample
AVA Vulnerability assessment	AVA_CCA					1	2	2		
	AVA_MSU			1	2	2	3	3	3	Analysis and testing of insecure states
	AVA_SOF		1	1	1	1	1	1	1	Strength of TOE security function evaluation
	AVA_VLA		1	1	2	3	4	4	4	Highly resistant

Annex 2. Evaluated product references

[ST]	Reference security target for the evaluation: - Project Chinook - Security Target of S3FS9CI 32-bit RISC Microcontroller For S-SIM, Version 1.7, 28th May 2008 Samsung Electronics Co. Ltd For the needs of publication, the following security target has been provided and validated in the evaluation: - Security Target Lite of S3FS9CI 32-bit RISC Microcontroller For S-SIM, Version 1.0, 4th June 2008 Samsung Electronics Co. Ltd
[ETR]	Evaluation technical report: - Chinook – Evaluation Technical Report, Reference: LETI.CESTI.CHI.RTE.001 - v1.0 - 29/05/2008, CESTI LETI For the needs of composite evaluation with this microcontroller a technical report for composition has been validated: - Chinook project - Evaluation Technical Report – lite, Reference: CESTI.LETI.CHI.ETR.002, Version 1.1 CESTI LETI
[CONF]	Project < CHINOOK >, Configuration Management Documentation (Class ACM_AUT/CAP/SCP), Version 1.5, Issued on 27th May, 2008, Samsung Electronics Co. Ltd
[GUIDES]	Guidance of the product: - Project <CHINOOK> Guidance Documents (Class AGD), Version 1.4, Issued on 26th May 2008 Samsung Electronics Co. Ltd - User's manual – S3FS9CI – 32-bit CMOS Microcontroller for S-SIM, Revision 1.12, May 2008 Samsung Electronics Co. Ltd - Security Application Note - S3FS9CI, version 1.11 Samsung Electronics Co. Ltd - Application Note - RSA Crypto Library with TORNADO^{TM} V3.8S, Version 1.10, Samsung Electronics Co. Ltd - Application Note - DRNG Software Library, Version 3.0, Samsung Electronics Co. Ltd

	- Project Chinook - Test-Administrator's Guidance, Version 1.1, Issued on 12th March 2008 Samsung Electronics Co. Ltd
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0002-2001.*

Annex 3. Certification references

Decree number 2002-535 dated 18th April 2002 related to the security evaluations and certifications for information technology products and systems.	
[CER/P/01]	Procedure CER/P/01 - Certification of the security provided by IT products and systems, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. The content of Common Criteria version 2.3 is identical to the international ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. The content of CEM version 2.3 is identical to the international ISO/IEC 18045:2005.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2007-04-001 version 2.3, revision 1, April 2007.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.
[REF-CRY]	Cryptographic mechanisms - Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms with standard robustness level version 1.10, 14th of September 2007, No. 1904/SGDN/DCSSI/SDS/LCR

[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004, Bundesamt für Sicherheit in der Informationstechnik