PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Certification report 2006/29

IC Platform of FeliCa Contactless Smartcard CXD9861/ MB94RS402 with HAL-API & DRNG Library

Paris, the 14th of December 2006

The Central-Director for Information Systems Security

Patrick Pailloux

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.

In case of disagreements, only the French version of this report is deemed authentic.

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.pm.gouv.fr

Certification report reference

2006/29

Product name

IC Platform of FeliCa Contactless Smartcard CXD9861/ MB94RS402 with HAL-API & DRNG Library

Product reference

IC version FR00 001, HAL-API v. 22.0, DRNG Library v. 22.0

Protection profile conformity

BSI-PP-02

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(s)

Fujitsu

1-1 Kamikodanaka 4_Chome, Nakahara-Ku, Kawasaki 211-8588 Japan

Sponsor

Fujitsu

1-1 Kamikodanaka 4_Chome, Nakahara-Ku, Kawasaki 211-8588 Japan

Evaluation facility

CEACI (Thales Security Systems – CNES)

18 avenue Edouard Belin, 31401 Toulouse Cedex 9, France

Phone: +33 (0)5 62 88 28 01, email : ceaci@cnes.fr

Recognition arrangements

CCRA

SOG-IS

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 « IC Platform of FeliCa Contactless Smartcard CXD9861/ MB94RS402 with HAL-API & DRNG Library , IC version FR00 001, HAL-API v. 22.0, DRNG Library v. 22.0 » developed by Fujitsu.

This product is a Platform Contactless Smartcard for communication purpose, it carries the application system for transportation and finance. It is in conformity with ISO/IEC18092 "Passive Communication Mode of Contactless communication interface (212/424kbps)".

1.2. Evaluated product description

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operation environment. Technical references used in this report are identified in the security target.

1.2.1. Product identification

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

- Smartcard Integrated Circuit "CXD9861/MB94RS402, version FR00 001"
- HAL-API version 22.0
- DRNG Library version 22.0

The product is physically identified by the identification characters and codes drawn with the top metal layer:

- Chip identification character
- Sony RC-S960
- FR00 MB94RS402

Plus the Hardware revision code on three Digit.
The product is labelled with different consistent labels are: MB94RS402, CXD9861, FR00 001.

1.2.2. Security services

The product provides mainly the following security services:

- SF.RNG: Deterministic Random Number Generator (DRNG) which generates 64bit random numbers.
- SF.DES: DES Co-processor, which is in conformance with FIPS46-3, supplies 1-key DES processing and 2-key triple-DES processing and supports the ECB or CBC mode, encryption and decryption.
- SF.Mal-Detect: Sensor functions that detect when the product is used outside the scope of defined environment such as abnormal temperature, frequency and voltage.

- SF.Phy-Detect: Active shield which detects the physical modification of the product in order to protect the TOE against physical-probing and physical-manipulation.
- SF.Phy-Protect: Physical layout that protects the product from physical manipulation and physical probing and make difficult to attack.
- SF.TEST: IC testing is performed by the Test features including IC Dedicated Test software and Test circuits in order to assure the correct operation of product function and the quality of product operation. Once IC testing is completed, Test features are invalidated.
- SF.Identification: Ability to write each product identification data on FRAM and pre-personalization data.
- SF.Memory-Access: Detection when the malicious software code performs unauthorized access to the product and the DMA access data is modified deliberately, in order to prevent disclose of the confidential data.
- SF.Memory-Scramble: Protection of confidential data stored in product memory areas against the manipulation and probing attacks. This function scrambles memory address data logically and makes difficult to read the memory data physically from outside.
- SF.Memory-Verification: CRC function to assure the integrity of FRAM data.

1.2.3. Architecture

The product consists of hardware part:
- CPU F2MC-8FX (8-bit CISC at 6.78 MHz)
- Memory (48KB ROM, 3KB SRAM, 9KB FRAM)
- DES Coprocessor
- DMA controller
- Analog circuit

The product also includes software :
- HAL-API (Hardware Abstraction Layer Application Program Interface)
- DRNG Library

1.2.4. Life cycle

Life Cycle of the product is be categorised to seven phases as in [BSI-PP-002]:
- Phase1: Smartcard Embedded Software Development
- Phase2: IC Development
- Phase3: IC Manufacturing
- Phase4 and Phase5: Smartcard production
- Phase6: Smartcard personalization
- Phase7: End-user

The product is developed in the different sites listed bellow.

IC development site in phase 2

Fujitsu ltd. Kawasaki R&D Facilities

4-1-1, Kamikodanaka, Nakaharaku, Kawasaki, Kanagawa, 211-8588, Japan.

Test program development site in phase 2

Fujitsu ltd. Akiruno Technology Center

50 Fuchigami, Akiruno, Tokyo, 197-0833, Japan

Mask manufacturing site in phase 2

Dai Nippon Printing Limited. Kamifukuoka plant

2-2-1, Fukuoka, Kamifukuoka-shi, Saitama 356-8507 Japan

IC Manufacturing site in phase 3

Fujitsu ltd. Mie plant

1500, Mizono, Todo-cho, Kuwana-shi, Mie-Ken, 511-0192, Japan

In the evaluation context, the IC Developer, IC Manufacturer, IC Packaging Manufacturer, Smartcard Product manufacturer, Personaliser, Smartcard Issuer have been considered as “product administrator” and the Smartcard Embedded Software developer has been considered as “product user”.

1.2.5. Evaluated configuration

This certification report applies to the microcontroller and software identified in §1.2.1 and described in §1.2.3. Any other software used for the evaluation are not part of the scope of certification.
With regard to the life-cycle, the evaluated product is the one at the end of its manufacturing phase (phase 3).

2. The evaluation

2.1. Evaluation referential

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

In order to meet the specificities of smart cards, the [CCIC] and [CCAP] guides have been applied.

2.2. Evaluation work

The evaluation technical report [RTE], delivered to DCSSI the 1st December 2006, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are "**pass**".

3. Certification

3.1. Conclusion

The evaluation identified in chapter 2 and described in the evaluation technical report [ETR], was carried out according to the current rules and standards, with the required competency and impartiality by 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 "IC Platform of FeliCa Contactless Smartcard CXD9861/ MB94RS402 with HAL-API & DRNG Library , IC version FR00 001, HAL-API v. 22.0, DRNG Library v. 22.0" 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 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] and shall respect the recommendations in the guidance [GUIDES] and the delivery document [DEL], in particular:

- The application developer shall give attention to the naming rules of the ROM code files exchanged with the IC developer, as they will be used for the identification of the final product.
- The application developer shall make sure its software complies with the guidance security requirements.

3.3. Recognition of the certificate

3.3.1. European recognition (SOG-IS)

This certificate is released 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:

3.3.2. International common criteria recognition (CCRA)

This certificate is released in accordance with the provisions of the CCRA [CC RA]. However, it is only recognised for EAL4 level.

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries[2], 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 SOG-IS agreement are: Finland, France, Germany, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.
2 The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, The Netherlands, New Zealand, Norway, Singapore, Spain, Sweden, Turkey, United Kingdom and United States.

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 : - IC Platform of FeliCa Contactless Smartcard CXD9861 / MB94RS402 Security Target, Version 5, Level 7, 13 Nov 2006. For the needs of publication, the following security target has been provided and validated in the evaluation: - IC Platform of FeliCa Contactless Smartcard CXD9861 / MB94RS402 Security Target (Public Version), Version 5, Level 3, Nov 22, 2006
[RTE]	Evaluation technical report : - Evaluation Technical Report Project: CXD9861 / MB94RS402, Ref.: TOR_ETR Revision : 2.0, 1 Dec. 2006. For the needs of composite evaluation with this microcontroller a technical report for composition has been validated: - ETR LITE for composition CXD9861 / MB94RS402, TOR_ETR_Lite, version 1.0, 1 Dec. 2006.
[CONF]	Configuration list of the product: - CM list for CC, v30 - Configuration list of the project - Project HAL Configuration list FR00 001(CS), 16 Nov 2006 - Project Submission List Version 34
[DEL]	ADO - DEL / ROM data acceptance manual 2 - 10-08-2006 / YT
[GUIDES]	Guidance of the product: - RC-S960 / MB94RS402 LSI Specifications, MB94RS402_USR_E01, V5L6 - HAL-API Function Specification, MB94RS402_USR_E02, V5L4 - DRNG Library Specifications, MB94RS402_USR_E03, V5L2
[PP-BSI-02]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certified 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.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, version 2.0, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, version 2.1, April 2006.
[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.