PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2008/15

IC Platform of FeliCa Contactless Smartcard CXD9916H3 / MB94RS403 & HAL Library

Paris, 26th of May 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

Certification report reference

DCSSI-2008/15

Product name

IC Platform of FeliCa Contactless Smartcard CXD9916H3 / MB94RS403 & HAL Library

Product reference

IC platform reference: CXD9916H3/MB94RS403 Version FR01 0001

Software library reference: HAL Library Version 01

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

Fujitsu Microelectronics Limited

1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki, 211-8588, Japan

Sponsor

Fujitsu Microelectronics Limited

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 61 28 16 51, 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 the IC Platform of FeliCa Contactless Smartcard CXD9916H3 / MB94RS403 & HAL Library developed by Fujitsu Microelectronics Limited.

An IC platform aims to host one or several software 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.

This IC platform is particularly designed for Felica Contactless Smartcard (communication, transportation and finance). It is in conformity with ISO/IEC18092 Passive Communication Mode of Contactless communication interface (212/424 kbps).

1.2. Evaluated product description

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operation environment.
This security target is compliant to [PP0002] protection profile.

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:

- IC platform reference: CXD9916H3/MB94RS403 Version FR01 0001;
- Software library reference: HAL Library Version 01.

The product is physically marked by identification code on the top metal layer. The HAL library offers also a command that allows retrieving identification information. These identification data are detailed in the Evaluation technical report for composition (cf. [ETR]).

1.2.2. Security services

The product provides mainly the following security services:

- 64 bits deterministic random number generator (DRNG);
- DES Co-processor conformant with FIPS46-3, supporting the ECB and CBC mode, encryption and decryption;
- Sensor functions that detect when the TOE is used outside the scope of defined environment such as abnormal temperature, frequency and voltage;
- Active shield which detects the physical modification of the TOE in order to protect the TOE against physical-probing and physical-manipulation;
- Physical layout that protects the TOE from physical manipulation and physical probing and make difficult to attack, protection against side-channel leakage;
- IC testing;

- Writing of identification and pre-personalization data in FRAM memory;
- Memory access control;
- Memory scrambling;
- FRAM integrity control.

1.2.3. Architecture

The CXD9916H3 / MB94RS403 product is made up of:

- A Hardware part:
  - An 8-bit CISC processing unit F^2MC-8FX ;
  - Memories: FRAM (4KB with integrity control), ROM (56KB) and SRAM (3KB) ;
  - Security Modules: Memory Access Control, memories integrity control, security sensors (voltage, frequency and temperature);
  - Functional Modules: I/O management in contactless mode “ISO/IEC 18092 Passive Communication Mode (212/424 kbps)”, support to Random Number Generation, DES co-processing units.
- A dedicated software is embedded in ROM which comprises:
  - HAL (Hardware Abstraction Layer) library including the 64bits deterministic random number generator (conformant to ANSIX9.42-2001 Annex C.2);
  - IC dedicated software (tests).

1.2.4. Life cycle

The product's life cycle is organised as follow:

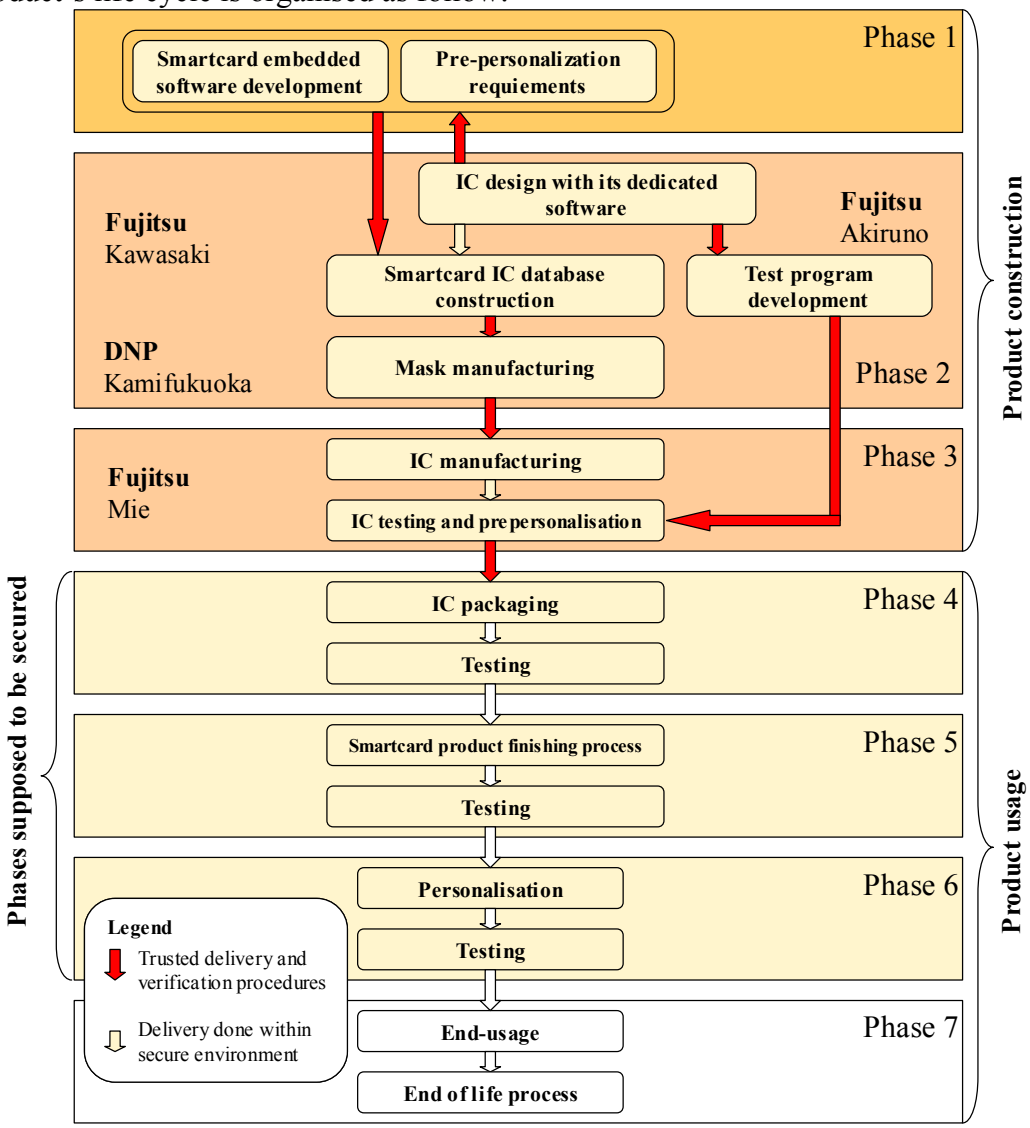

Figure 1 – Life cycle

The product is designed by:

Fujitsu Microelectronics Limited - Kawasaki R&D Facilities

1-1, Kamikodanaka 4-chome, Nakahara-ku,
Kawasaki, 211-8588,
Japan

The test program is developed by:

Fujitsu Microelectronics Limited - Akiruno Technology Center

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

The photo masks of the product are manufactured by:

Dai Nippon Printing Limited - Kamifukuoka plant

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

The product is manufactured and tested by:

Fujitsu Microelectronics Limited - Mie plant

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

The product can be in one of its two 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. Personalization data is loaded in the FRAM. The TOE configuration is changed to "user" by wafer sawing (test features are destroyed) 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 and software identified in §1.2.1 and described in §1.2.3. Any other software used for the evaluation is 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] 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 of the "IC Platform of FeliCa Contactless Smartcard CXD9861/ MB94RS402 with HAL-API & DRNG Library" product certified the 14th of December 2006 under the reference 2006/29 (cf. [2006/29]).

The evaluation technical report [ETR], delivered to DCSSI the 21st of May 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 evaluated the deterministic random number generator with the [AIS 20] methodology and 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]*)*, and meets the functionality class K3 and the strength of mechanism "high" of [AIS 20] .

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 "IC Platform of FeliCa Contactless Smartcard CXD9916H3 / MB94RS403 & HAL Library" 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 CXD9916H3 / MB94RS403 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:

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

[2006/29]	Certification report 2006/29 - IC Platform of FeliCa Contactless Smartcard CXD9861/ MB94RS402 with HAL-API & DRNG Library, 14th of December 2006, DCSSI.
[ST]	Reference security target for the evaluation: - IC Platform of FeliCa Contactless Smartcard CXD9916H3 / MB94RS403 - Security Target, Reference: MB94RS403_ST_E02_V6, May 20th, 2008 Fujitsu Microelectronics Limited For the needs of publication, the following security target has been provided and validated in the evaluation: - IC Platform of FeliCa Contactless Smartcard CXD9916H3 / MB94RS403 - Security Target (Public Version), Référence : MB94RS403_STlite_E02_V2, May 20th, 2008 Fujitsu Microelectronics Limited
[ETR]	Evaluation technical report : - Evaluation Technical Report - Project: TORNADO MINI, Reference: TORM_ETR_V4.0 CEACI For the needs of composite evaluation with this microcontroller a technical report for composition has been validated: - ETR LITE for composition TORNADO MINI - Smartcard Integrated Circuit "CXD9916H3/MB94RS403" / FR01 - HAL Library Version 01, Reference: TORM_ETR_Lite_V1.0 CEACI
[CONF]	The configuration list of the product is made of: - HAL configuration list V5L15, Reference: Tornado_HAL_CM_list_V5L15, Fujitsu Microelectronics Limited - Hardware configuration item lists 09/04/08, Reference: 20080404_CIL, Fujitsu Microelectronics Limited - MB94RS403 Configuration lists for CC document, 2008/5/20, version 14 Fujitsu Microelectronics Limited
[GUIDES]	The guidance of the product are made of: - CXD9916H3/MB94RS403 LSI Specification, Reference: MB94RS403_USR_E05_V3, Nov. 20, 2007, Fujitsu Microelectronics Limited - MB94RS403 HAL Library Specification, Reference: MB94RS403_USR_E04_V3, March 27, 2008 Fujitsu Microelectronics Limited

	- MB94RS403 Security Recommendation Guidance, Reference: MB94RS403_SRG_E01_V1, May 12, 2008, Fujitsu Microelectronics Limited
[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
[AIS 20]	Functionality classes and evaluation methodology for deterministic random number generators, AIS 20, Version 1,02/12/1999, Bundesamt für Sicherheit in der Informationstechnik