Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2008/18

Sony FeliCa Contactless Smart Card IC Chip RC-S962/1

Paris, 27th of June 2008

Courtesy Translation

SÉCURITÉ CERTIFICATION

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-2008/18

Product name

Sony FeliCa Contactless Smart Card IC Chip RC-S962/1

Product reference

RC-S962/1

Protection profile conformity

None

Evaluation criteria and version

Common Criteria version 2.3

compliant with ISO 15408:2005

Evaluation level

EAL 4

Developers

Sony Corporation

1-11-1 Osaki Shinagawa-ku, Tokyo, 141-0032, Japan

Fujitsu

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

Sponsor

Sony Corporation

1-11-1 Osaki Shinagawa-ku, Tokyo, 141-0032, 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 Sony FeliCa Contactless Smart Card IC Chip RC-S962/1 developed by Sony Corporation.

This smart card has multiple possible usages, covering needs of application in the fields of finance, for instance.

1.2. Evaluated product description

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

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:

- Commercial name: IC Chip RC-S962/1;
- Software reference : FeliCa OS version 3.31;
- Product ROM reference: 01 (with no patch);
- Microcontroller reference : CXD9916H3/MB94RS403 Version FR01 0001;
- Microcontroller dedicated software references: HAL Library Version 01.

The product can be physically identified by the identification codes visible on the top metal layer, and logically identified using the commands described in the guidance (see [GUIDES]).

1.2.2. Security services

The product provides mainly the following security services:

- Access control;
- Sequence control;
- Protection to confidentiality of communication data;
- Protection to integrity of communication data;
- Protection to integrity of internal data.

1.2.3. Architecture

The product consists of a microcontroller and dedicated software on which the operating system FeliCa OS is embedded, as summed up in the following picture.

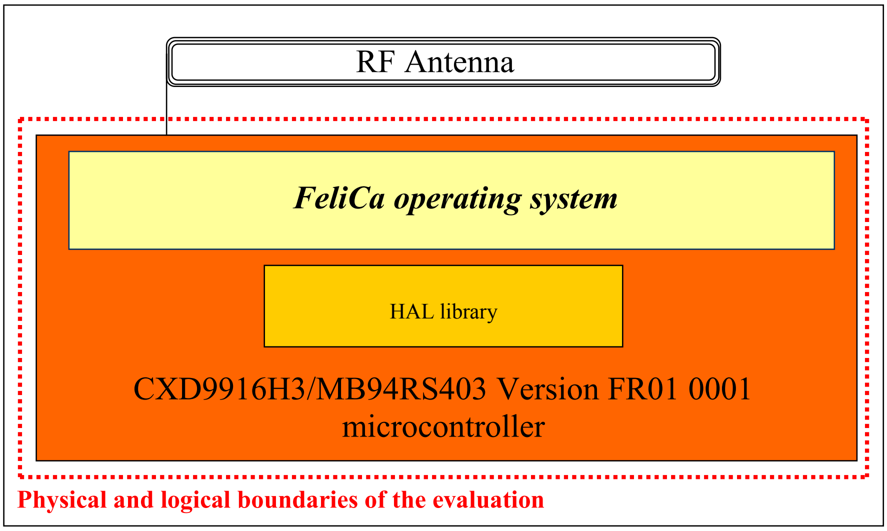
RF Antenna
FeliCa operating system
HAL library
CXD9916H3/MB94RS403 Version FR01 0001 microcontroller
Physical and logical boundaries of the evaluation

Figure 1 – Product architecture

1.2.4. Life cycle

The product's life cycle is organised as follow:

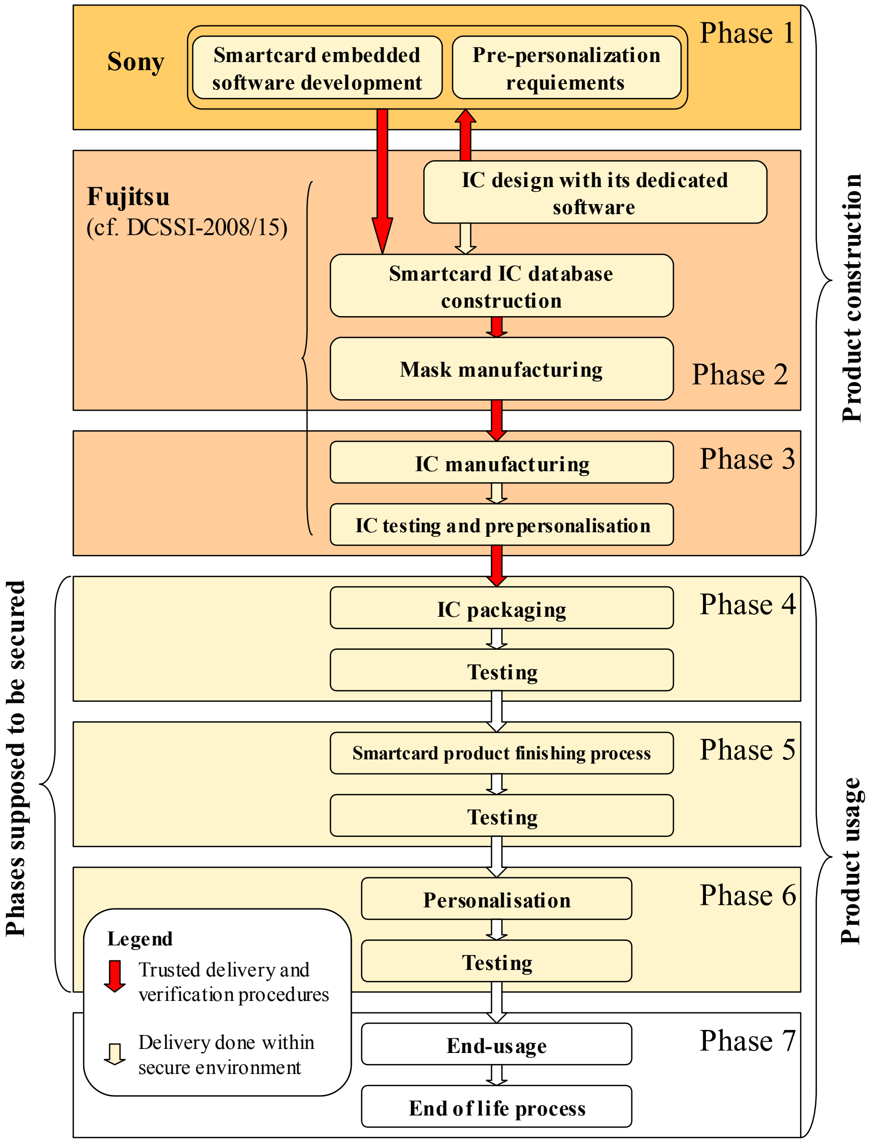
Sony
Smartcard embedded software development
Pre-personalization requiements
Phase 1
Fujitsu
(cf. DCSSI-2008/15)
IC design with its dedicated software
Smartcard IC database construction
Mask manufacturing
Phase 2
IC manufacturing
IC testing and prepersonalisation
Phase 3
Product construction
IC packaging
Testing
Phase 4
Smartcard product finishing process
Testing
Phase 5
Personalisation
Testing
Phase 6
End-usage
End of life process
Phase 7
Product usage
Phases supposed to be secured
Legend
Trusted delivery and verification procedures
Delivery done within secure environment

Figure 2 – Life cycle

The product is designed by:

Sony Gate City Osaki Office

1-11-1 Osaki Shinagawa-ku,
Tokyo, 141-0032,
Japan

The product is delivered via:

Sony Toyosato Plant

130 Koguchimae, Toyosato-cho, Tome-shi,
Miyagi-ken. 987-0362,
Japan

The microcontroller is designed and manufactured by:

Fujitsu Microelectronics Limited

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

1.2.5. Evaluated configuration

This certification report applies to the microcontroller and its embedded 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].

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 has been performed according to the composition scheme as defined in the guide [COMP] in order to assess that no weakness is introduced from the integration of the software in the microcontroller already certified.
Therefore, the results of the evaluation of the microcontroller “CXD9916H3/MB94RS403 Version FR01 0001” at EAL4 level augmented with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4, compliant with the [PP0002] protection profile, have been used. This microcontroller has been certified the 26th of May under the reference DCSSI-2008/15 (cf. [2008/15]).

The evaluation relies on the evaluation results of the Sony FeliCa Contactless Smart Card IC Chip RC-S960/1 product certified the 28th of June 2007 under the reference 2007/14 (cf. [2007/14]).

The evaluation technical report [ETR], delivered to DCSSI the 11th 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.

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 “Sony FeliCa Contactless Smart Card IC Chip RC-S962/1” submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL4.

3.2. Restrictions

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

The user of the certified product shall respect the operational environmental security objectives summarized specified in the security target [ST] chapter 4.2.2 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

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4	Intitulé du composant
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	1	Subset of the 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	1	Identification 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	2	Validation of analysis
	AVA_SOF		1	1	1	1	1	1	1	Strength of TOE security function evaluation
	AVA_VLA		1	1	2	3	4	4	2	Independent vulnerability analysis

Annex 2. Evaluated product references

[2007/14]	Certification Report DCSSI-2007/14 - Sony FeliCa Contactless Smart Card IC Chip RC-S960/1, 28th of June 2007, SGDN/DCSSI.
[2008/15]	Certification Report DCSSI-2008/15 - IC Platform of FeliCa Contactless Smartcard CXD9916H3 / MB94RS403 & HAL Library, 26th of May 2008, SGDN/DCSSI.
[ST]	Reference security target for the evaluation: - RC-S962/1 Composite Security Target, Reference: 962-ST-E01-10 version 1.10, Sony Corporation. For the needs of publication, the following security target has been provided and validated in the evaluation: - RC-S962/1 Composite Security Target – Public version, Reference: 962-STL-E01-10 version 1.10, Sony Corporation.
[ETR]	Evaluation Technical Report - Project: TYPHON-PETIT, Reference: TYPP_ETR_v1.0 CEACI
[CONF]	RC-S962 Configuration Management List, Reference: 962-CML-E01-10 version 1.10, Sony Corporation.
[GUIDES]	Delivery guidance: - Felica Card IC - RC-S962 IC Delivery Rules, Reference: No.962-DEL_IC-E01-20 version 1.20 Sony Corporation. Administration and user guidance: - FeliCa Card IC Security Operation Guidelines, Reference: M292-E0.1-00 version 1.0, Sony Corporation. - FeliCa Card Rewriting Transport key, Reference: Tec01-E01-10 version 1.1, Sony Corporation. - RC-S962 Series Inspection/Verification Procedure, Reference: M427-E01-00 version 1.0, Sony Corporation. - RC-S962 Series FeliCa OS Command Reference Manual, Reference: M417-E01-00 version 1.0, Sony Corporation. - RC-S962 Series FeliCa OS Status Flag Reference, Reference: M418-E01-00 version 1.0, Sony Corporation.

	- RC-S962 Series Manufacture ID Writing Procedure, Reference: M428-E01-00 version 1.0, Sony Corporation.
[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-2008-04-001 version 2.5 revision 1, April 2008.
[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