Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Certification report ANSSI-CC-2017/44

FeliCa Multi-interface Smart Card IC RC-SA08/1 and RC-SA08/2 (Version 1.00)

Paris,

COURTESY TRANSLATION

Warning

This report is intended to provide people who request evaluations with a document to certify the level of security provided by the product under the usage or operating conditions defined in this report for the version which was evaluated. It is also intended to provide potential acquirers of the product with the conditions under which they may use the product to ensure that they meet the conditions for which the product was evaluated and certified; this is why the certification report must be read in conjunction with the evaluated usage and administration guides and with the product's security target which describes the pre-supposed threats, environmental hypotheses and usage conditions so that the user can judge whether the product is suitable for their needs in terms of security objectives.

The certification does not in itself constitute a product recommendation by the agence nationale de la sécurité des systèmes d'information (ANSSI) and does not guarantee that the certified product is completely free of vulnerabilities that can be exploited.

All correspondence relating to this report must be sent to:

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Certification report reference

ANSSI-CC-2017/44

Product name

FeliCa Multi-interface Smart Card IC
RC-SA08/1 and RC-SA08/2

Product reference/version

Version 1.00

Conformity with a protection profile

[PP 0084], version 1.0
Security IC Platform Protection Profile with Augmentation Packages

Evaluation criteria and version

Common Criteria version 3.1 revision 4

Evaluation level

EAL 5 augmenté
ASE_TSS.2, ALC_DVS.2, AVA_VAN.5

Developers

Sony Corporation
Sony City Osaki 2-10-1 Osaki Shinagawa-ku
Tokyo, 141-86-10 Japan

STMicroelectronics
190 avenue Celestin Coq, ZI de Rousset,
13106 Rousset, France

Request made by

Sony Corporation
Sony City Osaki 2-10-1 Osaki Shinagawa-ku Tokyo, 141-8610 Japan

Evaluation centre

Serma Safety & Security
14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Applicable recognition agreements

CCRA

This certificate is recognised at EAL2.

SOG-IS

Foreword

Certification

Certification of the security provided by information technology products and systems is governed by amended decree 2002-535 of 18th April 2002. This decree indicates that:

- The agence nationale de la sécurité des systèmes d'information drafts the **certification reports**. These reports specify the characteristics of the security objectives proposed. They may contain any warnings that their authors consider are worth mentioning for security reasons. The people who order the reports may choose whether or not to communicate them to third parties or to make them public (article 7).
- The **certificates** awarded by the French Prime Minister certify that the individual product or system submitted for evaluation meets the specified security characteristics. They also certify that the evaluations were carried out according to current rules and standards, with the required levels of competence and impartiality (article 8).

The certification procedures are available on the website www.ssi.gouv.fr.

Table of contents

1. The product

1.1. Presentation of the product

The product evaluated is “FeliCa Multi-interface Smart Card IC RC-SA08/1 and RC-SA08/2, Version 1.00” developed by SONY CORPORATION and STMICROELECTRONICS. The product is a microcontroller with the embedded operating system FeliCa OS.

The microcontroller on its own is not a product that may be used in its current state. It is intended to host one or more applications. It may be inserted into a plastic support to constitute a smart card. This card has multiple uses (secure identity documents, banking applications, subscription television, transport, health, etc.) depending on the application software embedded in it. This software is not part of this evaluation.

1.2. Description of the product

1.2.1. Introduction

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

This security target complies with the protection profile [PP0084].

1.2.2. Security services

The main security services provided by the product are:

- the integrity and confidentiality protection of the user data and the embedded software executed or stored in the various memories of the TOE[1];
- the successful execution of the security services provided by the TOE;
- support for cryptographic encryption with symmetric or asymmetric keys;
- support for the generation of unpredictable random numbers.

1.2.3. Architecture

The product is composed of the following elements (see FIG. 1):

- the IC component ST31G480 developed by STMICROELECTRONICS, previously certified under the reference [ANSSI-CC-2016/58];
- the operating system FeliCa OS developer by SONY CORPORATION;
- a JavaCard platform outside the scope of the evaluation;
- Java applications outside the scope of the evaluation.

[1] *Target Of Evaluation*

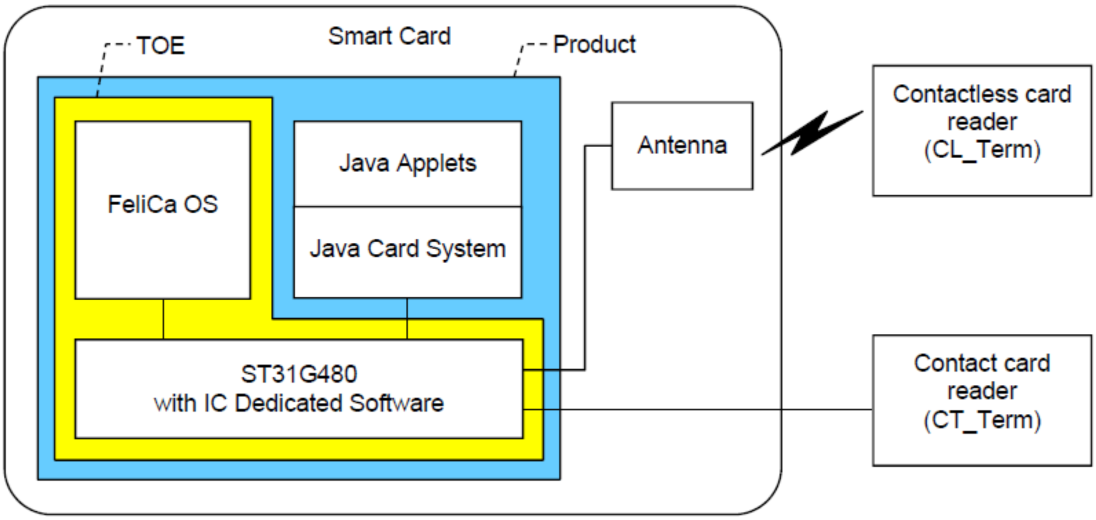
TOE
Smart Card
Product
FeliCa OS
Java Applets
Java Card System
ST31G480
with IC Dedicated Software
Antenna
Contactless card reader (CL_Term)
Contact card reader (CT_Term)

Figure 1 Product Architecture

The two configurations RC-SA08/1 and RC-SA08/2 differ only in their supported input capacitances, respectively 68 pF and 20 pF.

1.2.4. Product identification

The product's components are identified in the configuration list [CONF].

The certified product version is identified by the elements in the table below. These items can be verified by sending a specific command as specified in [GUIDES].

Configuration Items		Identification Data
FeliCa OS	*IC Type*	0x3E
	Rom Type	0x03
Microcontroller ST31G480 rev H	*Hardware identifier*	0x4248
	Firmware version	0x02 01 00 04

1.2.5. Life cycle

The product life cycle is as follows:

Phase	Description
Phase 1	*IC embedded software development*
Phase 2	*IC development*
Phase 3	*IC manufacturing*
Phase 4	*IC packaging*
	TOE delivery
Phase 5	*Composite product integration*
Phase 6	*Personalisation*
Phase 7	*Operational usage*

Delivery of the TOE is made at the end of phase 4.

The product was developed on the following site:

Development site

Sony City Osaki
2-10-1 Osaki, Shinagawa-ku, Tokyo, 141-8610
Japan

Logistic site

8-4 Shiomi, Kisarazu, Chiba, 292-0834
Japan

The development sites of the IC component are covered by the certificate [ANSSI-CC-2016/58].

1.2.6. Evaluated configuration

The certificate shall cover the microcontroller as defined in Chapter 1.2.4.

2. Evaluation

2.1. Evaluation reference bases

The evaluation was carried out according to **Common Criteria version 3.1 revision 4** [CC], and the evaluation methodology defined in the CEM manual [CEM].
For the assurance components which are not covered by the [CEM] manual, methods specific to the evaluation centre and validated by the ANSSI were used.

The guides [JIWG IC] and [JIWG AP] were applied to meet the specifics of the smart cards. So, the AVA_VAN level was determined according to the rating scale in the guide [JIWG AP]. Remember that this rating scale is more demanding than the scale defined by default in the standard method [CC], used for the other product categories (software products, for example).

2.2. Evaluation work

The evaluation in composition was carried out applying the guide [COMP] to check that no weaknesses are introduced by integrating the application into the microcontroller which has already been certified.
This evaluation therefore took into account the results of the evaluation on the microcontroller "ST31G480 A02 including optional cryptographic library NESLIB and optional technologies MIFARE DESFire EV1 and MIFARE Plus X" in EAL5 level augmented with the components ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_FLR.1, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, AVA_VAN.5 and ASE_TSS.2, in accordance with the protection profile [PP0084]. This microcontroller was certified on 25 August 2016 under the reference ANSSI-CC-2016/58.

The evaluation technical report [ETR], which was delivered to the ANSSI on 13 July 2017, details the work carried out by the evaluation centre and certifies that all the evaluation tasks are rated as "**success**".

2.3. Cryptographic mechanisms rating according to the ANSSI's technical reference bases

The cryptographic mechanisms were not rated according to the ANSSI's technical reference base [REF]. Nevertheless, the evaluation did not highlight any design or construction vulnerabilities for the AVA_VAN.5 level targeted.

2.4. Random number

2.5. Number generator analysis

The physical random number generator used by the final product was evaluated as part of the microcontroller evaluation (see [ANSSI-CC-2016/58]).

In addition, as required in the ANSSI's cryptographic reference base [REF], the output of the physical random number generator is subjected to cryptographic reprocessing.
The results were taken into account in the independent vulnerability analysis carried out by the evaluator and did not highlight any vulnerabilities that could be exploited for the AVA_VAN.5 level targeted.

3. Certification

3.1. Conclusion

The evaluation was carried out according to current rules and standards with the levels of competence and impartiality required for an approved evaluation centre. All of the evaluation work carried out enables a certificate to be issued according to decree 2002-535.

This certificate confirms that the product “FeliCa Multi-interface Smart Card IC RC-SA08/1 and RC-SA08/2, Version 1.00” submitted for evaluation meets the security characteristics specified in its security target [ST] for the evaluation level EAL 5 augmenté of the ASE_TSS.2, ALC_DVS.2, AVA_VAN.5 components.

3.2. Usage restrictions

This certificate relates to the product specified in chapter 1.2 of this certification report.

This certificate provides an assessment of the FeliCa Multi-interface Smart Card IC RC-SA08/1 and RC-SA08/2, Version 1.00 product's resistance to attacks which are highly generic due to the lack of a specific embedded application. Consequently, the security of a full product built on the micro-circuit may only be assessed by evaluating the full product; this evaluation may be carried out based on the results of the evaluation mentioned in chapter 2.

The user of the certified product must ensure that the security objectives are met within the operating environment, as specified in the security target [ST] and follow the recommendations in the guides provided [GUIDES].

3.3. Certificate recognition

3.3.1. European recognition (SOG-IS)

This certificate is issued under the conditions of the SOG-IS agreement [SOG-IS].

The 2010 SOG-IS European recognition agreement enables recognition of the ITSEC and Common Criteria certificates by the countries which have signed the agreement[1]. For smart cards and similar mechanisms, European recognition applies up to ITSEC E6 High and CC EAL7 level. The certificates that are recognised in the context of this agreement are issued with the following mark:

The 2010 SOG-IS European recognition agreement enables recognition of the ITSEC and Common Criteria certificates by the countries which have signed the agreement[2]. European recognition applies up to ITSEC E3 Elementary and CC EAL4 level. The certificates that are recognised in the context of this agreement are issued with the following mark:

3.3.2. International common criteria recognition (CCRA)

This certificate is issued under the conditions of the CCRA agreement [CC RA].

The "Common Criteria Recognition Arrangement" enables recognition of the Common Criteria certificates by the signatory countries[3].
Recognition applies to CC EAL2 level assurance components and the ALC_FLR family. The certificates that are recognised in the context of this agreement are issued with the following mark:

[1] The list of signatory countries of the SOG-IS agreement is available on the website www.sogis.org.

[2] The list of signatory countries of the SOG-IS agreement is available on the website www.sogis.org.

[3] The list of signatory countries of the CCRA arrangement is available on the website www.commoncriteriaportal.org.

Appendix 1. Product evaluation level

Class	Family	Components by assurance level							Assurance level selected for the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Component title
ADV **Development**	ADV_ARC		1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	1	Implementation representation of the TSF
	ADV_INT					2	3	3	2	Well-structured internals
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	4	Semiformal modular design
AGD **User guides**	AGD_OPE	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	Preparative procedures
ALC **Life cycle support**	ALC_CMC	1	2	3	4	4	5	5	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	5	Development tools CM coverage
	ALC_DEL		1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			1	1	1	1	2	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	2	Compliance with implementation standards
ASE **Security target evaluation**	ASE_CCL	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	2	TOE summary specification with architectural design summary
ATE **Tests**	ATE_COV		1	2	2	2	3	3	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	3	Testing: modular 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 estimation**	AVA_VAN	1	2	2	3	4	5	5	5	Advanced methodical vulnerability analysis

Appendix 2. Documentary references for the product evaluated

[ST]	Reference security target for the evaluation: - Security Target RC-SA08/01 and RC-SA08/02, Version 1.51, reference: A08-ST-E01-51, SONY CORPORATION. For publication requirements, the following security target has been supplied and validated in the context of this evaluation: - Security Target RC-SA08/1 and RC-SA08/2 – Public version, Version 1.51, reference: A08-STP-E01-51, SONY CORPORATION.
[RTE]	Technical evaluation report: - Evaluation Technical Report, Version 1.2, 13/07/2017, SERMA SAFETY AND SECURITY.
[CONF]	Product configuration list: - RC-SA08 Configuration List, Version 1.5, reference: A08-CML-E01-50, SONY CORPORATION.
[GUIDES]	- Product Acceptance Procedure, Version 1.0, reference: M985-E01-00, Sony Corporation; - RC-SA08 Inspection and IDm Writing Procedure, Version 0.9, reference: M1047-E00-90, SONY CORPORATION; - FeliCa Card User’s Manual, Version 1.02, reference: M660-E01-02, SONY CORPORATION.
[PP0084]	Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13 January 2014. *Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014.*
[ANSSI-CC-2016/58]	ST31G480 A02 including optional cryptographic library NESLIB and optional technologies MIFARE DESFire EV1 and MIFARE Plus X. *Certified by ANSSI on 25 August 2016 under the reference ANSSI-CC-2016/58.*

Appendix 3. References linked to certification

Amended decree No. 2002-535 of 18th April 2002 relating to the evaluation and certification of the security provided by information technology products and systems.	
[CER/P/01]	CER-P-01 procedure Certification of the security provided by information technology products and systems, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, September 2012, version 3.1, revision 4, ref CCMB-2012-09-001; Part 2: Security functional components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-002; Part 3: Security assurance components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, September 2012, version 3.1, revision 4, ref CCMB-2012-09-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, February 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smart cards, version 2.9, January 2013.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, January 2012.
[OPEN]	Certification of "Open" smart card products, version 1.1 (for trial use), 4 February 2013.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2, 2014.
[SOG-IS]	"Mutual Recognition Agreement of Information Technology Security Evaluation Certificates", version 3.0, 8 January 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), voir www.ssi.gouv.fr.

	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B3), voir www.ssi.gouv.fr.

*SOG-IS document; in the context of the CCRA recognition agreement, the equivalent CCRA support document applies.