Certification Report

RC-SA20, RC-SA21 and RC-SA24 Series version 1.00

Sponsor and developer: ***Sony Imaging Products & Solutions Inc.***
Sony City Osaki 2-10-1 Osaki
Shinagawa-ku, Tokyo, 141-8610
Japan

Evaluation facility: ***Brightsight***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-214607-CR**

Report version: **1**

Project number: **214607**

Author(s): **Wouter Slegers**

Date: **5 June 2020**

Number of pages: **12**

Number of appendices: **0**

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS:

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the RC-SA20, RC-SA21 and RC-SA24 Series version 1.00. The developer of the RC-SA20, RC-SA21 and RC-SA24 Series version 1.00 is Sony Imaging Products & Solutions Inc. located in Tokyo, Japan and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is an integrated circuit with a contactless interface and a smartcard embedded software called "FeliCa OS". The TOE is used as the public transportation IC card, e-money, identification card and so on.

The integrated circuit is the Fujitsu Semiconductor Limited chip CXD90056 and FeliCa OS is the FeliCa Operating System developed by Sony Imaging Products & Solutions Inc. including the application for services of the Service Provider.

All operations on the TOE are performed through a contactless card reader. Under the control of the FeliCa OS the TOE communicates with the contactless card reader according to ISO/IEC 18092 (Passive Communication Mode 212/424kbps).

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on June 5th, 2020 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the RC-SA20, RC-SA21 and RC-SA24 Series version 1.00, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the RC-SA20, RC-SA21 and RC-SA24 Series version 1.00 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]*[1] for this product provides sufficient evidence that the TOE meets the EAL6 augmented (EAL6+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ASE_TSS.2 (TOE summary specification with architectural design summary).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the RC-SA20, RC-SA21 and RC-SA24 Series version 1.00 from Sony Imaging Products & Solutions Inc. located in Tokyo, Japan.

The TOE is comprised of the following main components:

	Name	Version
Hardware	Fujitsu CXD90056 Smartcard IC – Hardware	20 00
Software	Fujitsu CXD90056 Smartcard IC – IC Dedicated Software	0B 00
	FeliCa Operating System 5.0	DF 0D

To ensure secure usage a set of guidance documents is provided together with the RC-SA20, RC-SA21 and RC-SA24 Series version 1.00. Details can be found in section 2.5 of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 1.3.

2.2 Security Policy

The TOE offers the following security features:

- mutual authentication between the external entity and the TOE
- authentication proof of the identity of the TOE to an external entity
- management of Services (e.g., setting Service Attribute)
- controlled access to the user data stored internally in the TOE
- trusted communication channel between the external entity and the TOE
- protection of confidentiality and integrity of assets stored internally in the TOE
- anti-tearing and rollback mechanism
- protection against excess environment conditions
- protection against information leakage
- protection against probing and alteration
- prevent abuse of function
- support of unique identification of the TOE.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The logical architecture, originating from the Security Target *[ST]* of the TOE can be depicted as follows:

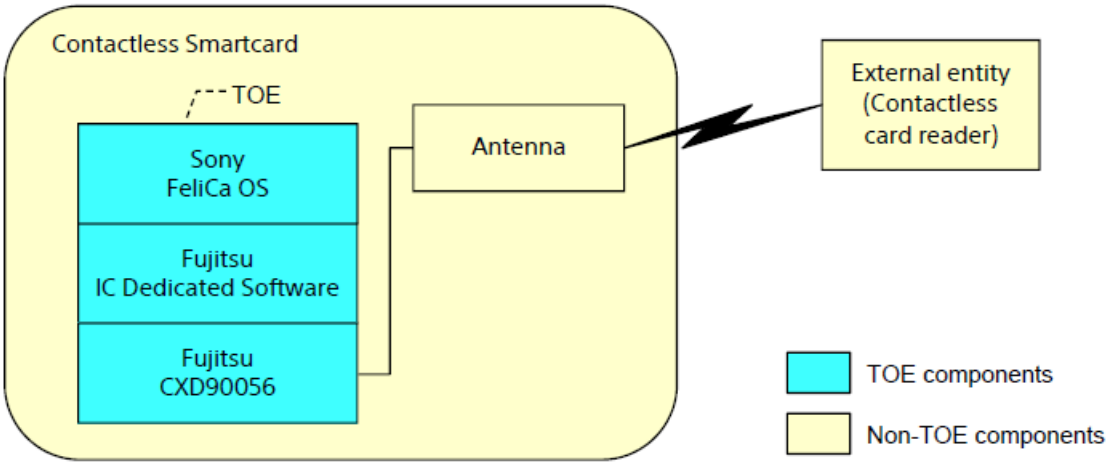

Figure 1. Logical architecture of the TOE.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Reference	Name	Version	Date
[AGD-PRE]	Sony Imaging Products & Solutions Inc, M985-E01-00 – Product Acceptance Procedure	1.0	February 2015
[AGD-CUM]	Sony Imaging Products & Solutions Inc, M660-E01-20 – FeliCa Card User's Manual	1.20	April 2020
[AGD-Insp-SA20]	Sony Imaging Products & Solutions Inc, M1125-E01-00 – RC-SA20 Series Inspection Procedure	1.00	May 2020
[AGD-Insp-ID-SA20]	Sony Imaging Products & Solutions Inc, M1123-E01-00 – RC-SA20 Series Inspection and Idm Writing Procedure	1.00	April 2020
[AGD-Insp-SA21]	Sony Imaging Products & Solutions Inc, M1126-E01-00 – RC-SA21 Series Inspection Procedure	1.00	May 2020
[AGD-Insp-ID-SA21]	Sony Imaging Products & Solutions Inc, M1124-E01-00 – RC-SA21 Series Inspection and Idm Writing Procedure	1.00	April 2020
[AGD-Insp-SA24]	Sony Imaging Products & Solutions Inc, Mxxxx-E01-00 – RC-SA24 Series Inspection Procedure	1.00	April 2020
[AGD-Insp-ID-SA24]	Sony Imaging Products & Solutions Inc, Mxxxx-E01-00 – RC-SA24 Series Inspection and Idm Writing Procedure-	1.00	April 2020
[AGD-SUM]	Sony Imaging Products & Solutions Inc, M1130-E00-90 –Secure ID User's Manual	0.90	April 2020
[AGD-Insp-SID]	Sony Imaging Products & Solutions Inc, M1131-E00-90 – RC-SA20, RC-SA21, RC-SA24 Series Secure ID Inspection Procedure	0.90	March 2020
[AGD-SRM-E1]	Sony Imaging Products & Solutions Inc, SRM-E01-E01-21 – Security Reference Manual – Group Key Generation (AES128bit)	1.21	February 2011
[AGD-SRM-E2]	Sony Imaging Products & Solutions Inc, SRM-E02-E01-21 – Security Reference Manual – Mutual Authentication & Secure Communication (AES128bit)	1.21	February 2011
[AGD-SRM-E3]	Sony Imaging Products & Solutions Inc, SRM-E03-E01-21 – Security Reference Manual –	1.21	February 2011

Reference	Name	Version	Date
	Package Generation (AES128bit)		
[AGD-SRM-E4]	Sony Imaging Products & Solutions Inc, SRM-E04-E01-21 – Security Reference Manual – Changing Key Package (AES128bit)	1.21	February 2011
[AGD-SRM-E5]	Sony Imaging Products & Solutions Inc, SRM-E05-E01-00 – Security Reference Manual – Group Key Generation for Communication with MAC (AES128bit)	1.00	March 2020
[AGD-SRM-E6]	Sony Imaging Products & Solutions Inc, SRM-E06-E01-00 – Security Reference Manual – Communication with MAC (AES128bit)	1.00	March 2020
[AGD-SRM-F1]	Sony Imaging Products & Solutions Inc, SRM-F01-E01-00 – Security Reference Manual – Secure ID	1.00	May 2020

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer uses a semi-automatic approach to derive test cases and perform testing. A Decision Table (DT) is created from the FeliCa specification and from the experience gained from previous projects. Automated tools are used to expand this decision table to cover all possible TSFI behaviour and to reach all module interfaces during testing, including all interesting boundary values. From the DT, test scripts are derived and the tests are executed. The resulting tests provide an extensive level of coverage and depth of testing.

For the hardware the test approach consists of four different types of testing:

- Simulation
- Lay-out check
- IC evaluation
- IC manufacturing test.

The functionality of each analogue and logic module is verified by simulation until an adequate coverage is reached. Subsequently they are tested on engineering samples and during manufacturing tests.

For the testing performed by the evaluators, the developer has provided samples and a test environment. The evaluators have reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent Penetration Testing

The methodical analysis performed was conducted along the following steps:

1. When evaluating the evidence in the classes ASE, ADV and AGD no potential vulnerabilities were identified from generating questions to the type of TOE and the specified behaviour.
2. For ADV_IMP a thorough implementation representation review was performed on the TOE. During this attack oriented analysis the protection against the attack scenarios was analysed using the knowledge gained from all previous evaluation classes. This resulted in the identification of additional potential vulnerabilities. This analysis was performed according to the attack list in [JIL-AM]. An important source for assurance against attacks in this step is the implementation review of the underlying platform; no additional potential vulnerabilities were concluded from this.

3. All potential vulnerabilities were analysed using the knowledge gained from all evaluation classes and the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. For most of the potential vulnerabilities a penetration test was defined. Several potential vulnerabilities were found to be not exploitable due to an impractical attack path.

In total, three penetration tests were performed, comprising two perturbation attacks and one side-channel attack for a total test effort of 5.5 weeks. One of the perturbation attacks was also an attack on the RNG.

2.6.3 Test Configuration

The TOE was tested in the following configuration:

- The hardware the tests were performed on ES2 which corresponds to HW version 0x0200, HAL version 0x0B00,
- Software used for testing was SW version 0xDF0D (little endian),
- IC Type 0x43, ROM type 0xF2. The ROM type is an identifier stored in FRAM, and was updated to "0x01" in the final product (this is the value listed in the *[ST]*).

This corresponds to RC-SA24 Series Version 1.00 as listed in the *[ST]* TOE reference.

2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e. from the current best cryptanalytic attacks published, has been taken into account.

The TOE supports key sizes (see *[ST]*) with sufficient algorithmic security level to exceed 100 bits as required for high attack potential (AVA_VAN.5).

2.7 Re-used evaluation results

There is no re-use of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number RC-SA20, RC-SA21 and RC-SA24 Series version 1.00. Verification of the TOE version is described in the guidance.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR],* which references a ASE Intermediate Report, Site Technical Audit Report(s) for the site(s) *[STAR-Sony], [STAR-Fujitsu], [STAR-DNP] and [STAR-ON]*[2] and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the RC-SA20, RC-SA21 and RC-SA24 Series version 1.00, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 6 augmented with ASE_TSS.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

[2] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

The Security Target claims 'strict' conformance to the Protection Profile *[PP]*.

Four sites have been audited as part of this evaluation and the results were described in STARs:

Site	STAR
Sony Sony City Osaki 2-10-1 Osaki Shinagawa-ku, Tokyo 141-8610 Japan	*[STAR-Sony]*
Fujitsu Shin-Yokohama TECH building 9-18, Shin-Yokohama 3-chome Kouhoku-ku Yokohama Japan	*[STAR-Fujitsu]*
DNP 2 Chome 2-1 Fukuoka Fujimino Saitama Japan	*[STAR-DNP]*
ON Semiconductors No. 6 Kogyo Danchi Monden-Machi Aizu Wakamatsu Fukushima Japan	*[STAR-ON]*

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE.

In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: DES legacy services.

3 Security Target

The Security Target RC-SA20, RC-SA21 and RC-SA24 Series, document reference SA2-ST-E01-02, version 1.02, dated April 2020 *[ST]* is included here by reference.

Please note that for the need of publication a public version *[ST-lite]* has been created and verified according to *[ST-SAN].*

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT security
PP	Protection Profile
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017.
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
[ETR]	Evaluation Technical Report “RC-SA20, RC-SA21 and RC-SA24 Series” EAL6+, 19-RPT-342, Version 6.0, Issue Date 02 June 2020.
[JIL-AM]	JIL, Attack Methods for Smartcards and Similar Devices (controlled distribution), Version 2.3, April 2019.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[PP]	Public Transportation IC Card Protection Profile, Version 1.12, 1 August 2018, certified by JISEC on 2018-09-04
[ST]	Security Target RC-SA20, RC-SA21 and RC-SA24 Series, document reference SA2-ST-E01-02, version 1.02, dated April 2020.
[ST-lite]	Security Target RC-SA20, RC-SA21 and RC-SA24 Series, Public version, SA2-STP-E01-02, v1.02
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.
[STAR-DNP]	Site Technical Audit Report DNP, document reference 19-RPT-278 v1.0, dated 29 November 2019, audit date May 29, 2019
[STAR-Fujitsu]	Site Technical Audit Report Fujitsu, document reference 19-RPT-272 v1.0, dated 21 November 2019, audit date May 22, 2019
[STAR-ON]	Site Technical Audit Report ON Semiconductor, document reference 19-RPT-276 v1.0, dated 27 November 2019, audit date May 27, 2019
[STAR-Sony]	Site Technical Audit Report Sony, document reference 19-RPT-274 v1.0, dated 21 November 2019, audit date May 24, 2019

(This is the end of this report).