Certification Report

JREM MN67S150-D Contactless Smart Card IC chip with fast processing function for transport

Sponsor:	***JR EAST MECHATRONICS CO., LTD.*** **Shinjuku Maynds Tower, 2-1-1, Yoyogi, Shibuya-ku,** **Tokyo, 151-0053** **Japan**
Developer:	***Sony Corporation*** **Sony City Osaki, 2-10-1 Shinagawa-kun,** **141-8610 Tokyo** **Japan**
Evaluation facility:	***Brightsight*** **Delftechpark 1** **2628 XJ Delft** **The Netherlands**
Report number:	**NSCIB-CC-10-30076-CR**
Report version:	**1**
Project number:	**NSCIB-CC-10-30076**
Authors(s):	**Wouter Slegers**
Date:	**June 4th, 2015**
Number of pages:	**14**
Number of appendices:	**0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Head office Apeldoorn:
Boogschutterstraat 11A
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

Location Apeldoorn:
Vissenstraat 6
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

Location Enschede:
Josink Esweg 10
P.O. Box 337
7500 AH Enschede
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 859

TÜV Rheinland Nederland B.V. is a
registered company with the
Amsterdam Chamber of Commerce
under number 27288788
info@nl.tuv.com
www.tuv.com/nl

Certificate

Standard

Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 4 (ISO/IEC 15408)

Certificate number **CC-10-30076**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder

JR EAST MECHATRONICS CO., LTD.

Shinjuku Maynds Tower, 2-1-1, Yoyogi, Shibuya-ku,
Tokyo, 151-0053, Japan

Developer

Sony Corporation

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

Product and assurance level

JREM MN67S150-D Contactless Smart Card IC chip with fast processing function for transport

Assurance Package:

- EAL6 augmented with ASE_TSS.2 in Advanced operation mode
- EAL4 in Backward-compatible operation mode

Project number **NSCIB-CC-10-30076-CR**

Evaluation facility

Brightsight BV located in Delft, the Netherlands

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 4 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL4

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 4 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 4. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

SOGIS
IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

Validity

Date of issue : **04-06-2015**
Certificate expiry : **04-06-2025**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

TÜV Rheinland Nederland B.V.
P.O. Box 541
7300 AM Apeldoorn
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

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 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 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.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

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 8 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.

Certificates issued before 08 September 2014 are still under recognition according to the rules of the previous CCRA (i.e. recognition based on assurance components up to and including EAL4+ALC_FLR). Also certification procedures started before 8 September 2014 and Assurance Continuity (maintenance and re-certification) of old certificates remain recognised according to the rules of the previous CCRA.

The certification of this product has started before 8 September 2014 and thus the recognition of the certificate falls under the recognition rules of the previous CCRA.

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 JREM MN67S150-D Contactless Smart Card IC chip with fast processing function for transport. The developer of the TOE is Sony Corporation located in Tokyo, Japan. The sponsor of the evaluation and certification is JR EAST MECHATRONICS CO., LTD. located in Tokyo, Japan. 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 Target of Evaluation – TOE (i.e., the JREM MN67S150-D Contactless Smart Card IC chip with fast processing function for transport) consists of the operating system, which is the Sony FeliCa Operating System, and the integrated circuit, which is the Panasonic Corporation (Panasonic) chip MN67S150.

The evaluation of the TOE was conducted as a composite evaluation and uses the results of the CC evaluation of the underlying hardware certified under the German CC Scheme on 16 April 2015 (*[HW CERT]*).

The TOE manages several data sets, each having a different purpose, on a single TOE. The TOE has a file system consisting of Areas and FeliCa Services, which organise files in a tree structure. Multiple Service Providers can use an Area or a FeliCa Service. Access keys enable access to data, via the Areas and FeliCa Services. This prevents unauthorised access to the User Services of other Service Providers. By organising these keys in a specific manner, multiple Area and FeliCa Services can be authenticated simultaneously.

The User Services are defined by Service Providers. A Service Provider, can incorporate the TOE into a ticketing system, to offer a ticket-payment User Service. A single TOE can be used by multiple Service Providers. A Service Provider can provide multiple User Services.

The TOE has been designed to support migration from a legacy infrastructure to a more secure infrastructure. To this end the TOE supports "Advanced" services that can be accessed using AES-protected authentication and read/write, and "Backward Compatible" services that can be accessed using DES-protected authentication and read/write.

To set up the User Services and the access to those services, the Administrator configures the TOE. This configuration work enables the TOE to offer various User Services, such as cash purse and transport-payment solutions. After the TOE is personalised, the Users are allowed only to access the FeliCa Services defined by the Administrator.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 15 May 2015 with the final delivery 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 FeliCa, 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 FeliCa 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]* for this product provide sufficient evidence that it 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). In Backwards-compatible mode the assurance is limited to EAL4.

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4 *[CEM*], for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 4 *[CC*].

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the JREM MN67S150-D Contactless Smart Card IC chip with fast processing function for transport 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.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the JREM MN67S150-D Contactless Smart Card IC chip with fast processing function for transport from JR EAST MECHATRONICS CO., LTD. located in Tokyo, Japan.

This report pertains to the TOE which is comprised of the following main components:

Type	Name	Release	Date	Form of delivery
Hardware platform				
IC hardware	Panasonic MN67S150 Smart Card IC in sawn wafer (die) form	RV08		Sawn wafer (dies)
IC Dedicated Software	Panasonic MN67S150 Smart Card IC – IC Dedicated Software	FV0C		Embedded in hardware
Software				
	FeliCa OS 5.0	3105		Embedded in hardware

To ensure secure usage a set of guidance documents is provided together with the FeliCa. Details can be found in section 2.5 of this report.

The TOE is delivered after Phase 3 of the *[PP].* For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 2.5.

For the correct identification of the TOE, the customer shall verify the correctness of the TOE by following Section 2.7 of *[AGD-INSP-IDM-PROC]* (Request Product Information command).

2.2 Security Policy

The TOE offers the following features:

- it can receive FeliCa formatted commands from the contactless interface
- it can send FeliCa formatted responses to the contactless interface
- it enables the set-up and maintenance of FeliCa Services by Service Providers
- it enables the use of FeliCa Services (e.g., decrement, cash-back)

The TOE offers the following security features:

- authentication of users
- controlled access to data stored internally in the TOE
- secure communication with the smartcard Reader/Writer
- protection of integrity of data stored internally in the TOE
- anti-tearing and rollback
- protection against excess environment conditions
- protection against information leakage
- protection against probing and alteration.

The security features are provided partly by the underlying hardware and partly by the FeliCa Operating System.

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. The following topics are of relevance (from the *[ST]*, chapter 3.2):

- A.Process-Sec-IC: Protection during Packaging, Finishing and Personalisation.

Furthermore, the following organisational security policy relates to the environment in which the TOE shall be operated (for the detailed and precise definition of the organisational security policy refer to the *[ST]*, chapter 3.3):

- P.Keys: The keys generated for TOE use shall be secure. The keys for use by the TOE shall be generated and handled in a secure manner.
- P.Plat-Appl: Usage of hardware platform.
- P.Resp-Appl: Treatment of user data.

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

This chapter provides a high-level description of the IT product and its major components based on the evaluation evidence described in the Common Criteria assurance family entitled “TOE design (ADV_TDS)”. The intent of this chapter is to characterise the degree of architectural separation of the major components.

The TOE is an integrated circuit for smart cards with an embedded smart card operating system. The operating system is the Sony FeliCa Operating System and the integrated circuit is the Panasonic chip MN67S150. The TOE form factor is a bare chip.

The following figure illustrates the TOE components and the physical scope of the TOE.

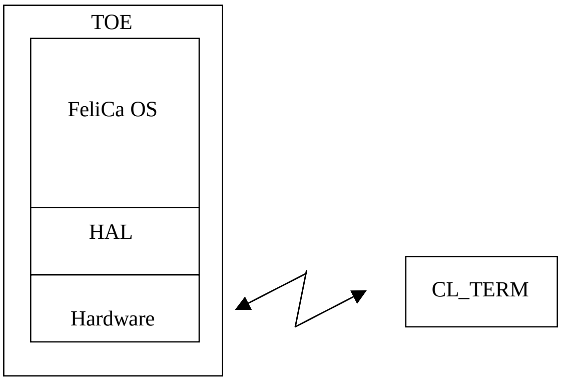

Figure 1: TOE physical scope

The “FeliCa OS” constitutes the part of the TOE that is responsible for managing and providing access to the User Areas and Services. “HAL” is the specific IC-dedicated software that controls and restricts access from the FeliCa OS to the hardware platform. “Hardware” is the hardware electronic platform of the TOE, which provides a contactless interface.

Under the control of the FeliCa Operating System the TOE integrated circuit communicates with a FeliCa RF card reader (CL_TERM) according to ISO/IEC 18092 (Passive Communication Mode 212/424kbps).

2.5 Documentation

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

Type	Name	Release	Date	Form of delivery
FeliCa				
Document	FeliCa Card User's Manual	1.02		Electronic document
Document	FeliCa OS for MN67S150 Inspection and IDm Writing Procedure	1.01		Electronic document
Document	FeliCa OS for MN67S150 Acceptance Procedure	1.00		Electronic document
Document	Security Reference Manual – Group Service Key & User Service Key Generation	1.00		Electronic document
Document	Security Reference Manual – Mutual Authentication & Packet Cryptography	1.01		Electronic document
Document	Security Reference Manual – Issuing Package Generation	1.00		Electronic document
Document	Security Reference Manual – Changing Key Package Generation	1.00		Electronic document
Document	Security Reference Manual – Group Key Generation (AES 128bit)	1.21		Electronic document
Document	Security Reference Manual – Mutual Authentication & Packet Cryptography (AES 128bit)	1.21		Electronic document
Document	Security Reference Manual – Issuing Package Generation (AES 128bit)	1.21		Electronic document
Document	Security Reference Manual – Changing Key Package Generation (AES 128bit)	1.21		Electronic document

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.

Note that the underlying hardware platform has been changed, re-evaluated, and certified in several steps, causing significant delays in this composite evaluation. To address these changes and the improvements in attack technology during these delays from the hardware certification, additional analyses and testing has been performed in this composite evaluation.

2.6.1 Testing approach and depth

The FeliCa OS running on Panasonic MN67S150 platform has been tested by Sony and the MN67S150 platform functions have been tested by Panasonic in the hardware evaluation.

The FeliCa OS has been tested on FSP, subsystem and module level. All parameter choices have been addressed at least once. The tests were largely automated, in a test suite for the FeliCa OS.

The developer has provided the evaluators with their test program and the full set of test scripts, and samples to perform the complete test set as defined by the developer, in addition to the tests defined by the evaluator.

The independent testing by the evaluator comprised of repeating a large subset of the developer's automated tests on the FeliCa OS tests on the TOE, covering all commands in the card-common specifications function as specified. These tests were repeated by the evaluator at the evaluator's premises.

In addition the evaluator performed independent testing in the context of ATE_IND.2-6. The evaluator has selected the following items to be tested for the FeliCa OS:

1. A test plan was made in which it was chosen to focus on the access control for different types of services;
2. A configuration was described containing three areas, each with public services, advanced services and backward compatible and each with chosen values for authentication keys.
3. In total 49 test cases were described in a test plan in which single services were authenticated in the chosen service configuration, combinations of services were authenticated and in which various negative tests were conducted;
4. Sony was asked to develop test scripts in which the service configuration could be installed on the TOE and in which the different test cases were performed;
5. The test scripts were analysed by the evaluator and discussed between the developer and evaluator for the expected results.
6. The test scripts were run by the evaluator on the developer supplied test configuration described above and verified.

To address the changes and delays in the certification of the hardware, analysis and limited retesting has been performed.

2.6.2 Independent Penetration Testing

The evaluator independent penetration tests were devised after performing an Evaluator Vulnerability Analysis. This was done in the following steps.

1. Inventory of required resistance
   This step used the JIL attack list *[JIL]* as a reference for completeness and studied the ST claims to decide which attacks in the JIL attack list applied for the TOE, as well as adding the evaluator's proprietary attack knowledge.
2. Validation of security functionalities
   This step identified the implemented security functionalities and performed evaluator independent tests to verify implementation and to validate proper functioning of the security functions.
3. Vulnerability analysis
   In this step the design and the implementation of the security functionalities was studied and an analysis was performed to determine whether the implementation potentially could be vulnerable against the attacks of step 1. Based on this analysis the evaluators determined whether the design and implementation provide sufficient assurance or whether penetration testing is needed to provide sufficient assurance.
4. Penetration testing
   This step performed the penetration tests identified in step 3.
5. Conclusions on resistance
   This step performed a *[JIL]* compliant rating on the results of the penetration tests in relation with the assurance already gained by the design analysis. Based on the ratings the evaluators made conclusions on the resistance of the TOE against attackers possessing a high attack potential.
6. To address the changes and delays in the certification of the hardware, these steps were revisited and a gap analysis was made, leading to additional analysis and tests, bringing the assurance on the TOE to the current state of the art.

2.6.3 Test Configuration

Testing by the evaluator was performed on the TOE in specific states suitable for testing (see *[ETR]* for details), which was analysed by the evaluation lab and was concluded to be applicable to all states of the TOE.

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.

2.7 Re-used evaluation results

Re-use has been made of evaluation results of a very similar TOE on another hardware platform under certification ID CC-13-37078.

Sites involved in the development and production of the hardware platform were re-used by composition. The development site has been visited as part of this evaluation: the Sony Development site on Floor 24 of the "Sony City Osaki" (SCO) building in Tokyo on October 2014.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number "JREM MN67S150-D Contactless Smart Card IC chip with fast processing function for transport". See the guidance (specifically *[AGD-INSP-IDM-PROC]*) for the proper verification procedure.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[1] which references several Intermediate Reports and other evaluator documents.

The verdict of al claimed assurance requirements is: **Pass**

Based on the above evaluation results the evaluation lab concluded the JREM MN67S150-D Contactless Smart Card IC chip with fast processing function for transport, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL6 augmented with ASE_TSS.2 in Advanced operation mode, and EAL4 in Backward-compatible operation mode**. This implies that the product satisfies the security technical requirements specified in the *[ST].*

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance.

The customer shall follow the provided guidance documentation. Please note that the documents contain relevant details with respect to the resistance against certain attacks.

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 implemented cryptographic algorithms was not rated in the course of this evaluation. To fend off attackers with high attack potential appropriate cryptographic algorithms with adequate key lengths must be used (references can be found in national and international documents and standards).

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

3 Security Target

The Security Target "JREM MN67S150-D Composite Security Target”, document F31-ST-E01-70, Revision 1.7, December 2014 is included here by reference.

Please note that for the need of publication a public version (F31-STP-E01-70) 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:

AES	Advanced Encryption Standard
DES	Data Encryption Standard
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
NSCIB	Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging
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:

[AGD-INSP-IDM-PROC] “FeliCa OS for MN67S150 Inspection and IDm Writing Procedure, Version 1.01

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, version 3.1 Revision 4.

[CEM] Common Methodology for Information Technology Security Evaluation, version 3.1, Revision 4.

[ETR] Evaluation Technical Report JREM MN67S150-D Contactless Smart Card IC chip with fast processing function for transport EAL6+, document reference 15-RPT-107, version 2.0, dated 2015-05-15

[ETR-HW] ETR for composite evaluation, EAL6, TUVIT, version 2, 2015-03-11

[HW CERT] Certification Report, BSI-DSZ-CC-0935-2015, MN67S150 Smart Card IC Version RV08 including IC dedicated software from Panasonic, 16 April 2015

[JIL] Attack methods for Smart cards and similar devices, JIL, Version 2.2, January 2013.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.1, August 1st, 2011.

[PP] "Security IC Platform Protection Profile", Version 1.0, June 2007, BSI-PP-0035

[ST] “JREM MN67S150-D Composite Security Target”, document F31-ST-E01-70, Revision 1.7, December 2014

[ST-HW] MN67S150 Panasonic Smart Card IC Security Target (ST-lite), version 1.8, 9 March 2015

[ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report).