Certification Report

FeliCa Contactless Smartcard IC RC-SA01/1 Series and RC-SA01/2 Series, version 1.0

Sponsor and developer: ***Sony Corporation***
1-7-1 Konan, Minato-ku, Tokyo
108-0075 JAPAN

Evaluation facility: ***Brightsight***
Delftechpark 1
2628 XJ Delft
The Netherlands

Report number: **NSCIB-CC-12-36329-CR**

Report version: **1**

Project number: **NSCIB-CC-12-36329**

Authors(s): **Wouter Slegers**

Date: **March 19, 2013**

Number of pages: **16**

Number of appendices: **0**

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 3 (ISO/IEC 15408)
Certificate number	**C12-36329**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**Sony Corporation** **Gotenyama Technology Center, 5-1-12 Kitashinagawa, Shinagawa-ku, 141-001 Tokyo, Japan**
Product and assurance level	**FeliCa Contactless Smartcard IC RC-SA01/1 Series and RC-SA01/2 Series version 1.0,** Assurance Package: ▪ EAL6 augmented with ASE_TSS.2 Protection Profile Conformance: ▪ Security IC Platform Protection Profile, Version 1.0, 15.06.2007; Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035
Project number	**NSCIB-CC-12-36329-CR**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 3 (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 3 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 3. 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.

Date of issue : **19-03-2013**

Certificate expiry : **19-03-2023**

Registration number

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

Managing Director
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.

A part of the procedure is the technical examination (evaluation) of the product 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 complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, 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 satisfies the security requirements.

Recognition of the certificate

The Common Criteria Recognition Arrangement and SOG-IS logos are printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

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 and approved certification schemes 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 FeliCa Contactless Smartcard IC RC-SA01/1 Series and RC-SA01/2 Series v1.0. The developer of the product is Sony Corporation 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.

This Certification Report is a “delta” with respect to the evaluation of the “FeliCa Contactless Smartcard IC RC-SA00/1 Series and RC-SA00/2 Series v1.0”. The changes are at the level of small changes to the implementation details, which results in the “Backward Compatible services” to be disabled for the TOE and the available memory to be different. The hardware and software are unchanged.

The Target of Evaluation - TOE (FeliCa Contactless Smartcard IC RC-SA01/1 Series and RC-SA01/2 Series v1.0) 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 Toshiba chip T6ND8. The TOE form factor is a bare chip.

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. For example, a public transport 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.

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 and was completed on February 18th, 2013 with the delivery of the final 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 certification was completed on March 19th, 2013 with the preparation of this Certification Report.

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 Contactless Smartcard IC RC-SA01/1 Series and RC-SA01/2 Series, 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 Contactless Smartcard IC RC-SA01/1 Series and RC-SA01/2 Series 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 provide sufficient evidence that it meets the EAL6 augmented with ASE_TSS.2 assurance requirements for the evaluated security functionality.

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 3 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the FeliCa Contactless Smartcard IC RC-SA01/1 Series and RC-SA01/2 Series v1.0 evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the

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

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 FeliCa Contactless Smartcard IC RC-SA01/1 Series and RC-SA01/2 Series v1.0 from Sony Corporation located in Tokyo, Japan.

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

Item	Identifier	Version	Medium
Hardware	Toshiba T6ND8 Smartcard IC – Hardware	6.0	Smartcard integrated circuit
Software	Toshiba T6ND8 Smartcard IC – IC Dedicated Software	4.0	Embedded in hardware
	FeliCa OS v5.0	3403, 3503	Embedded in hardware

The hardware is delivered in slight variations in input capacity and form factor, all of which are equivalent in security:

Product name	IC Code	Specifications
RC-SA01/1A	3403	8pF input capacity, 4KB EEPROM, bare chip with bump on wafer.
RC-SA01/1B		8pF input capacity, 4KB EEPROM, bare chip with bump in tray.
RC-SA01/1C		8pF input capacity, 4KB EEPROM, bare chip without bump on wafer.
RC-SA01/1D		8pF input capacity, 4KB EEPROM, bare chip without bump in tray.
RC-SA01/2A	3503	50pF input capacity, 4KB EEPROM, bare chip with bump on wafer.
RC-SA01/2B		50pF input capacity, 4KB EEPROM, bare chip with bump in tray.
RC-SA01/2C		50pF input capacity, 4KB EEPROM, bare chip without bump on wafer.
RC-SA01/2D		50pF input capacity, 4KB EEPROM, bare chip without bump in tray.

To ensure secure usage a set of guidance documents is provided together with the FeliCa Contactless Smartcard IC RC-SA01/1 Series and RC-SA01/2 Series. 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-PROC]* and *[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
- privacy protection against Card holder behaviour tracking
- 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 3.3):

- Ø 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 3.4):

- Ø 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.
- Ø P.Plat-Appl: Usage of hardware platform.
- Ø 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 (i.e., FeliCa Contactless Smartcard IC RC-SA01/1 Series and RC-SA01/2 Series) 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 Toshiba chip T6ND8. The TOE form factor is a bare chip.

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

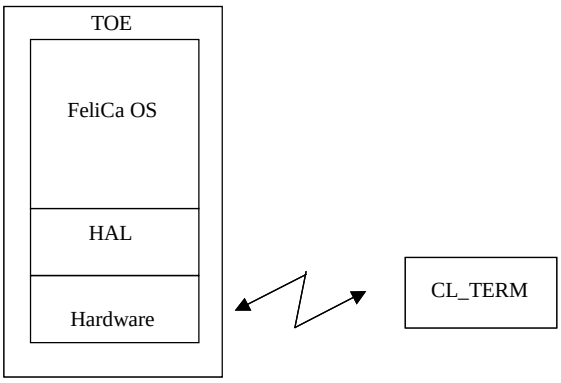

Figure 1: TOE physical scope

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:

Identifier	Version	Medium
FeliCa Card User’s Manual	1.01	Document
RC-SA01 Series Inspection Procedure	1.10	Document
RC-SA01 Series Inspection and IDm Writing Procedure	1.00	Document
RC-SA01 Series Acceptance Procedure	1.10	Document
FeliCa Card Application Note for Random ID	1.00	Document
Security Reference Manual – Group Key Generation (AES 128bit)	1.21	Document
Security Reference Manual – Mutual Authentication & Secure Communication (AES 128bit)	1.21	Document
Security Reference Manual – Package Generation (AES 128bit)	1.21	Document
Security Reference Manual – Changing Key Package Generation (AES 128bit)	1.21	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.

2.6.1 Testing approach and depth

The FeliCa OS running on T6ND8 platform has been tested by Sony and the T6ND8 platform functions have been tested by Toshiba. Both parts have been tested on FSP, subsystem and module level. All parameter choices have been addressed at least once. The tests were largely automated, in production testing for the hardware T6ND8 and 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 comprised of the evaluator repeating a large subset of the developer's automated tests on the FeliCa OS tests on the TOE and a small subset of the developer's tests on the T6ND8 platform functions in the context of ATE_IND.2-4 (this occurred in the context of the "FeliCa Contactless Smartcard IC RC-SA00/1 Series and RC-SA00/2 Series v1.0" evaluation). The rationale for this selection of the subsets is that testing the FeliCa OS extensively covers all relevant functionality of the T6ND8 platform, so only spot checking was necessary for the underlying T6ND8 platform. For the FeliCa OS, the tests that verify all commands in the card-common specifications function as specified were repeated by the evaluator at the evaluator premises. For the underlying T6ND8 platform the DES Crypto, AES crypto and CRC functionality were tested as part of the "FeliCa Contactless Smartcard IC RC-SA00/1 Series and RC-SA00/2 Series v1.0" evaluation.

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.

For the underlying T6ND8 platform testing included the following tests:

1. Active shield validation
2. Glue Logic validation
3. Validate DRNG seed entropy
4. Validation of TOT0/TOT1 protection in the DRNG seed
5. Validation of random wait states
6. Light sensor activation validation
7. RF communication logic behaviour validation

2.6.2 Independent Penetration Testing

The evaluator independent penetration tests were conducted according to the following testing approach:

During evaluation of the ADV, ATE and ALC classes the evaluators hypothesized possible vulnerabilities in the FeliCa OS. This resulted in a shortlist of possible vulnerabilities to be further analysed in AVA using the design knowledge gained in particular from the source code analysis in IMP and from the hardware ADV evaluation.

Next the evaluators analysed the TOE design and implementation for resistance against the [JIL] attacks. This resulted in further potential vulnerabilities to be tested.

The evaluators concluded that particular statements in four FeliCa commands - although well protected by the underlying chip hardware countermeasures - could be potentially vulnerable for perturbation using a high energy laser set up. Consequently a need for practical penetration testing was concluded for absolute assurance.

2.6.3 Test Configuration

Since the TOE's hardware component T6ND8 is not an end-user product it is not possible to perform testing without first embedding it in a testable configuration. To this end, the developer of the T6ND8 has created a proprietary test operating system. The main purpose of the test OS is to provide access to the HAL's functionality and was provided to the evaluators, and was used in the testing. The 8pf version of the hardware (IC Code 3203) was used for the tests (in the context of the "FeliCa Contactless Smartcard IC RC-SA00/1 Series and RC-SA00/2 Series v1.0" evaluation), with the exact ROM content and the settings for the TOE.

The full TOE is an end-user product and was tested as provided to the customer and as customized by the customer.

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

This security evaluation re-used the evaluation results of the recently performed evaluation of the "FeliCa Contactless Smartcard IC RC-SA00/1 Series and RC-SA00/2 Series v1.0" (i.e. slightly different settings for the software), certified on September 3rd, 2012 under the certification identifier NSCIB-10-30075.

On August 31th, 2012, Sony, the developer of the TOE submitted an application form to the NSCIB Certification Body requesting to issue a certificate for their FeliCa Contactless Smartcard IC RC-SA01/1 Series and RC-SA01/2 Series, version 1.0 product.

The changes between the previously certified "FeliCa Contactless Smartcard IC RC-SA00/1 Series and RC-SA00/2 Series v1.0" and " FeliCa Contactless Smartcard IC RC-SA01/1 Series and RC-SA01/2 Series, version 1.0" (the TOE) can be categorized as:

- A slightly different setting for the software (with identical hardware and software).
- Developer evidence updates as result of the above changes, including ST and Guidance Documents

The assessment of the update by the evaluation lab in the *[ETR]* indicated that the changes have no security issues and that the original evaluation results could be re-used. For added assurance, minor additional evaluator testing was performed and developer evidence was analyzed to get sufficient assurance that the changes have no effect on the security level of the TOE. The evaluation lab also confirmed in the *[ETR]* that the original Vulnerability Analysis performed on "FeliCa Contactless Smartcard IC RC-SA00/1 Series and RC-SA00/2 Series v1.0" is still valid.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number FeliCa Contactless Smartcard IC RC-SA01/1 Series and RC-SA01/2 Series v1.0. See the guidance (specifically *[AGD-INSP-CMD], [AGD-INSP-IDM-PROC] and [AGD-PRE]*) for the proper verification procedure.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]* which references several Intermediate Reports and other evaluator documents. The verdict of each claimed assurance requirement is given in the following tables:

Development		**Pass**
Security architecture	ADV_ARC.1	Pass

Functional specification	ADV_FSP.5	Pass
Implementation representation	ADV_IMP.2	Pass
TSF Internals	ADV_INT.3	Pass
Security policy modelling	ADV_SPM.1	Pass
TOE design	ADV_TDS.5	Pass

Guidance documents		**Pass**
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass

Life-cycle support		**Pass**
Configuration Management capabilities	ALC_CMC.5	Pass
Configuration Management scope	ALC_CMS.5	Pass
Delivery	ALC_DEL.1	Pass
Development security	ALC_DVS.2	Pass
Life-cycle definition	ALC_LCD.1	Pass
Tools and techniques	ALC_TAT.3	Pass

Security Target		**Pass**
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.2	Pass

Tests		**Pass**
Coverage	ATE_COV.3	Pass
Depth	ATE_DPT.3	Pass
Functional tests	ATE_FUN.2	Pass
Independent testing	ATE_IND.2	Pass

Vulnerability assessment		**Pass**
Vulnerability analysis	AVA_VAN.5	Pass

Based on the above evaluation results the evaluation lab concluded the FeliCa Contactless Smartcard IC RC-SA01/1 Series and RC-SA01/2 Series v1.0, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL6 augmented with ASE_TSS.2**. This implies that the product satisfies the security technical requirements specified in Security Target "Security Target FeliCa Contactless Smartcard IC RC-SA01/1 Series and RC-SA01/2 Series", document A01-ST-E01-10, version 1.10, November 2012.

The Security Target claims strict conformance to the Eurosmart, Security IC Platform Protection Profile BSI-PP-0035, version 1.0, 15.06.2007, registered and certified by BSI under the reference PP-0035.

2.10 Evaluator Comments/Recommendations

2.10.1 Obligations and hints for the developer

None.

2.10.2 Recommendations and hints for the customer

The customer shall follow the provided guidance documentation, in particular consider *[AGD-Idnote]* when using the FPR_UNL.1 unlinkability features.

3 Security Target

The Security Target "Security Target RC-SA01/1 Series and RC-SA01/2 Series", document A01-ST-E01-10, version 1.10, November 2012 is included here by reference.

Please note that the for the need of publication a public version (A01-STP-E01-10) 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
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
DRNG	Deterministic Random Number Generator
HAL	Hardware Abstraction Layar
IT	Information Technology
ITSEF	IT Security Evaluation Facility
NSCIB	Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging
OS	Operating System
PP	Protection Profile
RF	Radio Frequency
TOE	Target of Evaluation

5 Bibliography

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

[AGD-Idnote] FeliCa Card Application note for Random ID, v1.0

[AGD-INSP-IDM-PROC] RC-SA01 Series Inspection and IDm Writing Procedure, v1.0

[AGD-INSP-PROC] RC-SA01 Series Inspection Procedure, v1.10

[AGD-PRE] RC-SA01 Series Acceptance Procedure, v1.10

[AIS20] Application Notes and Interpretation of the Scheme (AIS), Functionality classes and evaluation methodology for deterministic random number generators by Certification body of the BSI, Section II 2, as part of the certification scheme, AIS 20 Version 1, December 2, 1999

[AIS34] AIS 34 Evaluation Methodology for CC Assurance Classes for EAL5+, version 3, 03.00.2009

[Attack] Attack methods for smart cards and similar devices, version 2, February 2011

[ARC] JIL, Security Architecture requirements (ADV_ARC) for Smart Cards JIL, and similar devices, Version 1.0 (for trial use), June 2008 [CC] Common Criteria for Information Technology Security Evaluation, Parts I version 3.1 revision 1, and Part II and III, version 3.1 revision 3.

[CEM] Common Methodology for Information Technology Security Evaluation, version 3.1, Revision 3, July 2009.

[COMPO] CCDB-2007-09-001, “Composite product evaluation for Smart Cards and similar devices”, Version 1.0 Revision 1, September 2007”

[ETR] Brightsight, Evaluation Technical Report Evaluation Technical Report FeliCa Contactless Smartcard IC FeliCa Contactless Smartcard IC RC-SA01/1 Series and RC-SA01/2 Series 1.0 EAL6+, 13-RPT-020, Version 2.0, February 18, 2013.

[INT] CCDB-2006-04-003, “Application of CC to Integrated Circuits”, Version 3.0, Revision 1, March 2009

[JIL] CCDB-2009-03-001, "Application of Attack Potential to Smart Cards”, version 2.7, March 2009

[JHAS] JIL, "Application of Attack Potential to Smart Cards”, version 2.8, January 2012

[NSCIB] Nederlands Schema for Certification in the Area of IT Security, Version 2.0, 1 July 2011.

[NSI1] NSCIB Scheme interpretation #1, Performing site audits, Version 1.9, 11 November 2008.

[NSI2] NSCIB Scheme interpretation #2, Composite evaluations, Version 1.9, 11 November 2008.

[NSI3] NSCIB Scheme interpretation #3 Performing Testing, Version 0.9

[NSI4] NSCIB Scheme interpretation #4 Cryptographic Assessments, Version 0.9

[PP] Eurosmart, Security IC Platform Protection Profile BSI-PP-0035, version 1.0, 15.06.2007

[ST] Security Target FeliCa Contactless Smartcard IC RC-SA01/1 Series and RC-SA01/2 Series, document A01-ST-E01-10, version 1.10, November 2012.

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

(This is the end of this report).