TNO CERTIFICATION

Laan van Westenenk 501
P.O. Box 541
7300 AM Apeldoorn
The Netherlands

Phone +31 55 5493468
Fax +31 55 5493288
E-mail: Certification@certi.tno.nl

BTW/VAT NR NL8003.32.167.B01
Bank ING at Delft
Bank account 66.77.18.141
stating 'TNO Certification'
BIC of the ING Bank: INGBNL2A
IBAN: NL81INGB0667718141

Date
June 24, 2009

Reference
NSCIB-CC-09-10991-CR

Subject

Project number
10991

NSCIB-CC-09-10991

Certification Report

Sony RC-S957/2 Series with contact-based operating system out of scope, v1.0

TNO CERTIFICATION

TNO CERTIFICATION
HEREBY DECLARES THAT EVALUATION
HAS DEMONSTRATED THAT THE PRODUCT

Sony RC-S957/2 Series with contact-based operating system out of scope, v1.0, Assurance Package: EAL4
Product and version

FROM

Sony Corporation located in Tokyo, Japan
Sponsor's name and address

COMPLIES WITH THE

Common Criteria for Information Technology Security Evaluation (CC), Version 2.3 (ISO/IEC 15408)

Certification guidelines or standards

AS DEMONSTRATED BY / EVALUATION PERFORMED BY

Brightsight BV located in Delft, the Netherlands
Testing Laboratory

APPLYING THE

Common Methodology for Information Technology Security Evaluation (CEM), Version 2.3 (ISO/IEC 18045)

NSCIB-CC-09-10991-CR
Certification Report number

THE CERTIFICATE HAS BEEN ISSUED ON

June 24, 2009
Date

June 24, 2019
Expiry Date

ISSUED IN: Apeldoorn, the Netherlands

DIRECTOR TNO CERTIFICATION

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 2.3 for conformance to the Common Criteria for IT Security Evaluation version 2.3. 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 TNO Certification or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TNO Certification or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

CERTIFICATE NUMBER C09-10991

ACCREDITED BY THE COUNCIL FOR ACCREDITATION

Table of contents

Table of contents 3
Document Information 3
Foreword 5
1 Executive Summary 6
2 Certification Results 8
2.1 Identification of Target of Evaluation 8
2.2 Security Policy 9
2.3 Assumptions and Clarification of Scope 9
2.3.1 Usage assumptions 9
2.3.2 Environmental assumptions 10
2.3.3 Clarification of scope 10
2.4 Architectural Information 10
2.5 Documentation 12
2.6 IT Product Testing 12
2.6.1 Testing approach 12
2.6.2 Test Configuration 12
2.6.3 Depth 13
2.6.4 Independent Penetration Testing 13
2.6.5 Testing Results 13
2.7 Evaluated Configuration 13
2.8 Results of the Evaluation 14
2.9 Evaluator Comments/Recommendations 15
2.9.1 Obligations and hints for the developer 15
2.9.2 Recommendations and hints for the customer 15
3 Security Target 16
4 Definitions 16
5 Bibliography 17

Document Information

Date of issue	24 June 2009
Author	R.T.M. Huisman
Version of report	1
Certification ID	NSCIB-CC-09-10991
Sponsor and Developer	Sony Corporation
Evaluation Lab	Brightsight BV
TOE name	RC-S957/2 Series with contact-based operating system out of scope, v1.0
Report title	Certification Report
Report reference name	NSCIB-CC-09-10991-CR

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, TNO Certification 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 TNO Certification in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF is a commercial facility that has been licensed by TNO Certification 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, TNO Certification 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 Recognition Agreement approved by the SOG-IS in April 1999 provides mutual recognition of ITSEC and Common Criteria certificates for all evaluation levels (E6, resp. EAL7). This agreement was originally signed by Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the RC-S957/2 Series with contact-based operating system out of scope, v1.0. The developer of the RC-S957/2 Series with contact-based operating system out of scope 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 security evaluation is a "delta" that re-uses the evaluation results of the recently performed evaluation of the original RC-S957 Series with contact-based operating system out of scope, v1.0. The original RC-S957 Series was certified on June 9th 2008 under the certification identifier NSCIB-07-09612. The difference between the original RC-S957 and this RC-S957/2 version of the TOE is that this certificate now includes a software update to correct a functional problem. The original certificate remains valid as this functional problem was solved there by a procedural workaround in the documentation.

The Target of Evaluation – TOE (i.e., RC-S957/2 Series with contact-based operating system out of scope) is a dual interface integrated circuit with an embedded smartcard operating system. The TOE is part of the RC-S957/2 Series product of Sony and has an Antenna Module form factor (IC with antenna). There are various types of antennas for RC-S957/2 Series, but this is not important here because the antenna is determined not to be security relevant. The RC-S957/2 Series product contains the FeliCa Operating System of Sony, the Global Platform Operating System (excluded from the TOE) and the integrated circuit AE45X1-C of Renesas *[ST-HW]*. The TOE contains the FeliCa Operating System, a small part of the Global Platform Operating System that implements the bootstrap and the Renesas integrated circuit. The evaluation of the TOE was therefore conducted as a composite evaluation and uses the results of the CC evaluation of the underlying Renesas AE45X1-C (HD65145X1) integrated circuit certified under BSI-DSZ-CC-0351-2006.

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 unauthorized access to the User Services of other Service Providers. By organizing these keys in a specific manner, multiple Area and FeliCa Services can be authenticated simultaneously. The security measures of the TOE aim at protecting the access to the User Services (including associated user data) and to maintain the confidentiality and integrity of the user data. The User Services are defined by Service Providers. For example, a public transport Service Provider can incorporate the RC-S957/2 Series product 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 two interfaces: contact-based and contactless. All operations on the TOE are performed through a card reader (either a contact-based or a contactless card reader). The card reader and the TOE authenticate each other, and only then shall the TOE allow the card reader access, according to the access policy defined by the Administrator. This policy is named Service Access Policy. After authentication the communication between the TOE and the card reader is encrypted (based on single DES).

The RC-S957/2 Series with contact-based operating system out of scope has several self-protection mechanisms, as follows:

- Common smartcard self-protection mechanisms, such as security sensors, protect the integrated circuit.
- Integrity mechanisms ensure the integrity of data is preserved and prevent bypassing of the

access control mechanism. On both start-up and any read access, a CRC check is performed on the database information.

- The writing of data to the database is an atomic operation.

The previous release of the TOE was originally evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on 29 May 2008. The current RC-S957/2 Series with contact operating system out of scope v1.0 has been re-evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on June 23th 2009 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 June 24th 2009 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 RC-S957/2 Series with contact operating system out of scope, 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-S957/2 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 EAL 4 (Evaluation Assurance Level 4) assurance requirements for the evaluated security functionality. The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 2.3 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 2.3 *[CC]*.

TNO Certification, as the NSCIB Certification Body, declares that the RC-S957/2 Series with contact operating system out of scope, v1.0 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 Assurance Level (EAL) 4 evaluation is the RC-S957/2 Series with contact operating system out of scope, v1.0 from Sony Corporation located in Tokyo, Japan.

This report pertains to the TOE which has the following form factor: Antenna Module (IC with antenna). There are various types of antennas for RC-S957/2 Series. The TOE is comprised of the following main components[2]:

Item	Identifier	Version
Hardware	Renesas AE45X1-C (HD65145X1)	03
Software	ROM Image comprising of: • ROM FeliCa Operating System, Dual OS v1.1 • ROM Global Platform OS, v2.0.1' with Boot control and Contactless dispatcher	0C06 06 2005-08-02

To ensure secure usage a set of guidance documents is provided together with the RC-S957/2 Series. Details can be found in section 2.5 of this report.

The life-cycle of the TOE is best explained using the smartcard life-cycle as defined in *[BSI-PP-0002]*, which includes the following phases:

- Phase 1 — Smartcard-embedded software developer
- Phase 2 — IC developer
- Phase 3 — IC manufacturer
- Phase 4 — IC packaging manufacturer
- Phase 5 — Smartcard product manufacturer
- Phase 6 — Personaliser
- Phase 7 — Smartcard issuer

The FeliCa Operating System (included in the TOE) and the Global Platform Operating System is developed in **Phase 1**. Sony delivers the smartcard-embedded software and its pre-personalisation data to Renesas. The IC (included in the TOE) is developed and manufactured in **Phase 2** and **Phase 3** by Renesas. In these phases the smartcard-embedded software and its pre-personalisation data are injected. After Phase 3 the IC including operating systems is delivered to Sony. In **Phase 4** the RC-S957/2 Series (Antenna Module) product is assembled by Sony. In **Phase 5** Sony delivers the RC-S957/2 Series product to the Administrator. The Administrator is responsible for personalisation (**Phase 6**) and finally delivers the product to the User (**Phase 7**).

[2] Please note: This report is a "delta" with respect to the evaluation of the "RC-S957 Series with contact operating system out of scope" with certification id NSCIB-07-09612. The difference between this evaluated TOE and the original RC-S957 is a small software change that corrects a functional problem and has no security impact. A further difference is the provided guidance documentation.

2.2 Security Policy

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 (as shown in Figure 1). 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 unauthorized access to the User Services of other Service Providers. By organizing these keys in a specific manner, multiple Area and FeliCa Services can be authenticated simultaneously.

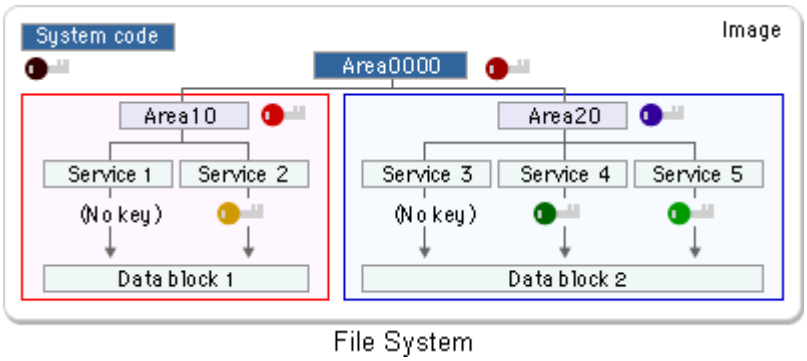

Figure 1 - FeliCa file system

The security measures of the TOE aim at protecting the access to the User Services (including associated user data) and to maintain the confidentiality and integrity of the user data. The User Services are defined by Service Providers. For example, a public transport Service Provider can incorporate the RC-S957/2 Series product into a ticketing system, to offer a ticket-payment User Service. A single TOE can be used by multiple Service Providers. Each Service Provider can provide multiple User Services.

The TOE has two interfaces: contact-based and contactless. All operations on the TOE are performed through a card reader (either a contact-based or a contactless card reader). The card reader and the TOE authenticate each other, and only then shall the TOE allow the card reader access, according to the access policy defined by the Administrator. This policy is named Service Access Policy. After authentication the communication between the TOE and the card reader is encrypted (based on single DES).

The RC-S957/2 Series with contact-based operating system out of scope has several self-protection mechanisms, as follows:

- Common smartcard self-protection mechanisms, such as security sensors, protect the integrated circuit.
- Integrity mechanisms ensure the integrity of data is preserved and prevent bypassing of the access control mechanism. On both start-up and any read access, a CRC check is performed on the database information.
- The writing of data to the database is an atomic operation.

2.3 Assumptions and Clarification of Scope

2.3.1 Usage assumptions

There are no usage assumptions identified in the Security Target that are of relevance to the TOE.

2.3.2 Environmental assumptions

The following assumptions about the environmental aspects defined by the Security Target have to be met (for the detailed and precise definition of the assumptions refer to the *[ST]*, chapter 3.2):

- The TOE assumes that the Global Platform OS is benign.
- It is assumed that security procedures are used between delivery of the TOE by the TOE Manufacturer and delivery to the User, to maintain the confidentiality and integrity of the TOE and its manufacturing and test data (to prevent any possible copying, modification, retention, theft or unauthorised use). This means that assets after TOE Delivery are assumed to be protected appropriately.
- It is assumed that all cryptographic keys generated outside the TOE are kept secret and secure.

2.3.3 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

Figure 2 presents the physical scope and boundaries of the TOE, which is indicated in green. The form factor RC-S957/2 Series of the TOE is indicated in yellow. The form factor of the smartcard is indicated in gray. The Global Platform OS, which is out of scope of the TOE, is indicated in blue.

The components of the TOE "FeliCa Operating System" constitute the part of the TOE that is responsible for managing and providing access to the Areas and Services. "Boot control" is the part of the TOE that is responsible for the start-up of the operating systems. "Contactless dispatcher" is the part of the TOE that is responsible for the processing of received commands, including those from the contact-based interface through the Global Platform OS. "Renesas AE45X1-C integrated circuit" is the hardware platform of the TOE, which provides a contact-based interface and a contactless interface. Via the interfaces, APDU and FeliCa commands are exchanged; these commands are processed by the FeliCa OS. The hardware has detectors, sensors, and circuitry to protect the TOE. The antenna provides the RF interface on the smartcard.

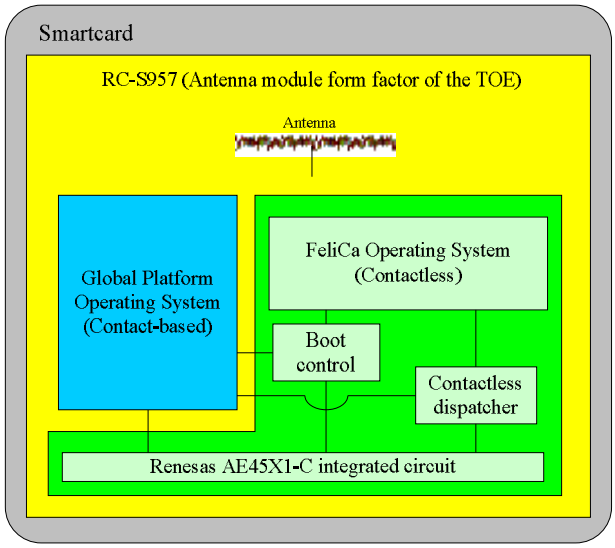

Figure 2, The RC-S957/2 Series product, showing the relationships between its internal components and external entities

The TOE contains the following security functions:

- SF1. Access Control and Authentication. This security function controls the access to the user data stored in the FeliCa file system and performs authentication between the FeliCa OS and the card readers. The TOE distinguishes between Users and Administrators.

  Operations that are allowed before successful identification and authentication are: Polling, Requests, Public_read, Public_write, and Echo Back. The TOE enforces the Service Access Policy by means of a list of area codes and service codes, which can be given to the TOE as part of a mutual authentication, specifies for which group of areas and services in the FeliCa file system authentication is requested. After successful mutual authentication the TOE has also agreed a Transaction Key with the card reader, which is the basis for secure communication and for the following operations on files by Users and Administrators: Authentication, Read, Write, Diagnosis, Requests, Echo Back, Decrement, and Cashback. A user can have access to a file only when that user is successfully authenticated and the requested operation is listed in the service access mode.

  The mutual authentication and the access control to specific user data are based on cryptographic operations of Triple-DES with 112-bit keys conformant to FIPS PUB 46-3. The mutual authentication includes a random number to prevent replay attacks (forging or copying of authentication data). The random numbers are conformant to K.3 of *[AIS20]*. The random number uses the random number generator of the underlying hardware, see *[ST-HW]*, to create a seed.

  This security function also includes secure Key Loading, which enables the concept of providing access to a group of Areas and FeliCa Services during authentication. Only the Administrator can set the Service Access Policy.

- SF2. Secure Communication. This function provides encipherment of information in interactions with external entities, to protect the confidentiality and integrity of information. The encryption and decryption is based on a DES CBC mode cipher using the 56-bit Transaction Key resulting from the mutual authentication. The cryptographic operations are conformant to FIPS PUB 46-3. The Transaction Key is conformant to FeliCa Technology. User information in secure communication also includes a MAC, a Random number, and a sequence number, to protect the integrity of user data and to protect against replay attacks.

- SF3. Secure Data Storage. This function ensures the integrity of user data stored in the FeliCa file system. This function provides a mechanism to ensure data integrity of data stored in EEPROM, based on the CRC checksum parameter stored in the file system for each block of user data and on the verification of that parameter.

- SF4. Anti-Tearing and Rollback. This function ensures that the writing of data is either successfully completed or rolled back to a consistent state. Anti-Tearing and Rollback is a protective mechanism to avoid loss of data integrity due to power loss during complex transactions. If power loss occurs during a complex transaction, all data modifications made during the transaction are rolled back.

- SF5. Protection Against Excess Environment Conditions. This function ensures the detection of tampering with the TOE due to environmental conditions, that is, physical manipulation and physical probing. This function is based on detectors and sensors on the integrated circuit, for protection of working conditions in which the TOE functions reliably and for protection against manipulation of external conditions (e.g., excess voltage) that cause the TOE to function in an unreliable manner. The TOE can react to excess environmental conditions by either resetting the chip or giving an error response to commands. The function relies on the security measures in the chip, as described in *[ST-HW]*.

- SF6. Protection Against Information Leakage. This function ensures the protection against information leakage from the TOE. This function is based on circuitry on the integrated circuit, to protect the TOE against leakage of information via side channels. Externally these protective mechanisms show as noise on the chip connectors. These protective mechanisms have scramble data. The function relies on the security measures in the chip, as described in *[ST-HW]*.
- SF7. Protection Against Probing and Alteration. This function ensures the protection against physical attacks from physical manipulation and physical probing. This function is based on circuitry on the integrated circuit, to protect the TOE against observation or tapping of TOE-internal data. This function also protects the TOE against physical alteration of chip circuitry that aims to weaken or by-pass security mechanisms.

2.5 Documentation

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

Identifier	Version
RC-S957A/2 Product Specifications	1.00
RC-S957A/2 Manufacture ID Writing Procedure	1.0
RC-S954 Series FeliCa OS Command Reference Manual	1.0
RC-S957 Series FeliCa OS Inspection/Initialization Command Specifications	2.0
FeliCa Card Rewriting Transport Key	1.1
FeliCa Card Cautions for Application Development	1.0
Cross Access Functional Specifications	1.0
RC-S954/2MV Cross Access Functional Specifications Errata	1.0
Security Reference Manual Group Service Key & User Service Key Generation Procedure	1.0
Security Reference Manual Mutual Authentication & Packet Cryptography	1.01
Security Reference Manual Issuing Package Generation	1.0
Security Reference Manual Changing Key Package	1.0

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

The independent testing comprised of confirming the developer testing by running all the developer's tests at the evaluator's site.

2.6.2 Test Configuration

The test configuration for the independent testing comprised of a PC equipped with Microsoft Windows 2000 running Cygwin 2.51.2.2 and the RC-S957/2 Test Suite. Also a reader/writer Sony RC-S440C/S460C (contactless FeliCa terminal) was used.

The test configuration for independent testing is the same as used for the functional testing by the developer.

2.6.3 Depth

Testing corresponded with the depth of the high-level design. The testing by the developer exercised all modules and all internal interfaces of the TOE. The TOE is tested in its default 'test' state. The whole test suite encompasses 2664 individual test which are performed in a single run taking about 4 hours (witnessed by the evaluator). The developer employed three basic testing techniques:

- Varying input (commands parameters and data), either by providing invalid input or invalid ordering of commands. Most test procedures used this technique and covered the security functions:
  - SF1. Access Control and Authentication
  - SF2. Secure Communication
- Varying the timing required to write to EEPROM to simulate power failure interrupts when saving critical data. These tests are designed to test the effectiveness of security function SF4 Anti-Tearing and Rollback.
- Loading a test program to change the content of EEPROM after writing/before reading to test the detection of data storage faults. These tests are designed to test the effectiveness of security function SF3 secure data storage.

For each command is tested how the TOE reacts in different modes, when it receives varying packet lengths, to test cases in which the command should not give a response. The functional tests by the developer do not cover the following security functions as these are provided by the hardware see *[ETR-HW]*:

- SF5. Protection Against Excess Environment Conditions
- SF6. Protection Against Information Leakage
- SF7. Protection Against Probing and Alteration

2.6.4 Independent Penetration Testing

The vulnerability analysis performed on the previous release of the TOE was based on an older version of *[JIL]*. The evaluator made an analysis of the differences between the two version and concluded that no new attacks were revealed nor that the attack potential rating was changed.

Due to the above the evaluator considers that the original TOE vulnerability analysis (which is at AVA_VLA.2 level) is still valid and does not need to be re-performed.

2.6.5 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. Residual vulnerabilities were found.

2.7 Evaluated Configuration

The TOE is defined uniquely by its name and version number RC-S957/2 Series with contact operating system out of scope, v1.0 and can be identified by its ROM version: 0C06 and form factor: Antenna Module (IC with antenna).

The TOE needs no specific configuration settings because there is only one configuration defined.

2.8 Results of the Evaluation

As part of the developer evidence, Sony Corporation as the developer of the RC-S957/2 Series with contact operating system out of scope, v1.0 submitted an Impact Analysis Report *[IAR]* to the NSCIB Certification Body requesting a new certificate for their updated product. The IAR is intended to satisfy the requirements outlined in the document Assurance Continuity: CCRA Requirements *[CCRA-AC]*. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes and the security impact of the changes.

The changes made to the TOE comprised minor modifications to the source code and the removal of a guidance document. With the modified software a functional problem is fixed and the work-around solution described in guidance "RC-S954 Series Important Notice" is no longer necessary.

The assessment of the IAR indicated that the original evaluation results could be re-used with minor modifications according to the following table:

Assurance class		Changed?	Impact
Security Target	ASE	Minor	TOE name and TOE delivery items have been changed.
Configuration Management	ACM_AUT.1	No	None
	ACM_CAP.4	Minor	Configuration list has been changed.
	ACM_SCP.2	Minor	Configuration list has been changed.
Delivery and Operation	ADO_DEL.1	No	None
	ADO_IGS.1	Minor	A guidance has been withdrawn.
Development	ADV_FSP.2	No	None
	ADV_HLD.2	No	None
	ADV_IMP.1	Minor	Source code has been changed to fix the bug.
	ADV_LLD.1	No	None
	ADV_RCR.1	No	None
	ADV_SPM.1	No	None
Guidance documents	AGD_ADM.1	Minor	The name of some documents has been changes.
	AGD_USR.1	Minor	The name of some documents has been changes.
Life cycle support	ALC_DVS.1	No	None
	ALC_LCD.1	No	None
	ALC_TAT.1	No	None
Tests	ATE_COV.2	No	None
	ATE_DPT.1	No	None
	ATE_FUN.1	Minor	New test results has been added.
	ATE_IND.2	No	None
Vulnerability assessment	AVA_MSU.2	No	None
	AVA_SOF.1	No	None

Assurance class		Changed?	Impact
	AVA_VLA.2	No	None

The evaluation lab confirmed in the *[ETR]*[3] that the IAR and updated evidence are complete and correct and that additional testing showed that the functional problem is fixed.

Based on the above evaluation results the evaluation lab concluded the RC-S957/2 Series with contact operating system out of scope, v1.0, to be **CC Part 2 conformant**, **CC Part 3 conformant**, and to meet the requirements of **EAL 4**. This implies that the product satisfies the security technical requirements specified in Security Target RC-S957/2 Series with contact-based operating system out of scope (957-2-ST-E01-10), version 1.1, May 2009. The Security Target does not claim conformance to any Protection Profile.

The Security Target makes a strength of function claim **SOF-medium**. The evaluation has shown that the TOE effectively fulfils this strength of function claim. Note that the SOF claim does not apply to the algorithmic strength of cryptographic mechanisms, with the exception of the random number security mechanism.

2.9 Evaluator Comments/Recommendations

2.9.1 Obligations and hints for the developer

Based on the insights gained during the evaluation the evaluator stresses the importance of the secure delivery of the TOE, i.e. that the process of delivering a TOE from the developer to the customer is executed conformant to the delivery procedures described in *[DEL-IC]*.

2.9.2 Recommendations and hints for the customer

Based on the insights gained during the evaluation the evaluator stress the importance of the following items:

- Strictly follow the cautions for application development as described in the guidance document 'FeliCa Card Cautions for Application Development', more specifically the caution to use only randomly generated keys and not to use the same key for two different services or areas.
- Initialise the TOE in a secure environment only and prevent exposure of the software library (see guidance document 'RC-S957 Series FeliCa OS Inspection/Initialization Library Specifications') to not-secured environments and limit personnel access to this software.

[3] 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 RC-S957/2 Series with contact-based operating system out of scope (957-2-ST-E01-10), version 1.1, May 2009 is included here by reference. Please note that for the need of publication a public version (957-2-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:

APDU	Application Protocol Data Unit
CC	Common Criteria
CRC	Cyclic Redundancy Check
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
SPA/DPA	Simple/Differential Power Analysis
TNO	Netherlands Organization for Applied Scientific Research
TOE	Target of Evaluation

5 Bibliography

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

[AIS20] AIS 20 (Version 1 of 2-12-1999): Functionality classes and evaluation methodology for deterministic random number generators.

[BSI-PP-0002] Eurosmart Smartcard IC Platform Protection Profile (BSI-PP-0002.), 1.0, July 2001.

[CCRA-AC] Assurance Continuity: CCRA Requirements, Common Criteria document CCIMB-2004-02-009, version 1.0, February 2004

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, August 2005, Version 2.3, CCIMB-2005-08-001/2/3.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, August 2005, Version 2.3, CCIMB-2005-08-004.

[DEL-IC] RC-S954 Series IC Delivery Rules (954-DEL_IC-E01-10), version 1.1, November 19, 2007.

[ETR] Evaluation Technical Report, RC-S957/2 Series with contact operating system out of scope (09-RPT-128), Version 2.0, June 23, 2009.

[ETR-HW] Renesas AE45X1-C ETR-Lite, version 1.0, July 13, 2007.

[JIL] JIL Application of Attack Potential to Smart Cards, version 2.61, September 2008.

[NSCIB] Nederlands Schema for Certification in the Area of IT Security, Version 1.2, 9 December 2004.

[ST] Security Target RC-S957/2 Series with contact-based operating system out of scope, version 1.1, May 2009.

[ST-HW] Renesas AE45X1-C (HD65145X1) Version 03 Smartcard Security Target – Public Version, Revision 4.0, August 3, 2007.

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