REF:	2008-13-INF-396 v2	Created:	TECNICO
Distrib:	Público	Reviewed:	TECNICO
Date:	26.11.2009	Approbed:	JEFEAREA

CERTIFICATION REPORT FOR RC-S251/SO2 v1.0

Dossier: 2008-13
Applicant data: 690553649Q SONY CORPORATION

References:

EXT-614	Certification Request of RC-S251/SO2 v1.0. 21/07/08. SONY Corporation.
EXT-826	Evaluation Report for TOE: RC-S251/SO2 v1.0 ETRSONY001 M3 01/09/09. LGAI-APPLUS.
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.
SOGIS	European Mutual Recognition Agreement of IT Security Evaluation Certificates version 2.0, April 1999.

Certification report of RC-S251/SO2 v1.0, as requested by SONY Corporation in [EXT-614] dated 21-7-2008, and evaluated by the laboratory LGAI-APPLUS, as detailed in the Evaluation Technical Report [EXT-826] received on September 1st 2009, and in compliance with [CCRA].

Table Of Contents

Executive Summary

This document constitutes the Certification Report for the composite product RC-S251/SO2 v1.0 developed by SONY Corporation on the integrated circuit IC for smart card AE57C1, manufactured by Renesas.

Developer/manufacturer: Sony Corporation.

Sponsor: Sony Corporation.

Certification Body: Centro Criptológico Nacional (CCN). Centro Nacional de Inteligencia (CNI).

ITSEF: LGAI Technological Center. APPLUS.

Protection Profile: none.

Evaluation Level: EAL4+ (AVA_VAN.5, ALC_DVS.2).

Evaluation end date: 01/09/2009.

All the assurance components required by the level EAL4+ (augmented with AVA_VAN.5, ALC_DVS.2) have been assigned a “PASS” verdict. Consequently, the laboratory (LGAI-APPLUS) assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4 methodology, as define by of the Common Criteria [CC-P3] and the Common Methodology [CEM].

Considering the obtained evidences during the instruction of the certification request of the RC-S251/SO2 v1.0 product on the integrated circuit for intelligent card AE57C1, a positive resolution is proposed.

During the execution of this smartcard evaluation the laboratory, responding to the CB’s demand, has used the additional requirements and guidance provided by the *JIL Working Group (JIWG)* in the form of *JIL papers* and *CC supporting documents* related to the IT domain of *Smartcards and similar devices*. The *Joint Interpretation Library (JIL)* supports the specific technical competence aspects required by the SOGIS MRA [SOGIS] in this field for several CC activities, specially beyond the EAL1-EAL4 levels covered by the CCRA.

These additional JIL references are mainly related to the evaluation of composite TOEs, and they are the documents listed below:

- [AAP] Application of Attack Potential to Smartcards v2.7
- [CPE] Composite product evaluation for Smart Cards and similar devices v1.0
- [SCG] Smartcard evaluation guidance v1.2
- [ARC] Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices v1.0 (trial)
- [CDE] Collection of Developer Evidence v1.1
- [AMS] Attack Methods for Smartcards and Similar Devices v1.5
- [RIC] Requirements to perform Integrated Circuit Evaluations v1.0

The CB was updating to the ITSEF with the last versions of these documents during the whole evaluation process.

TOE Summary

The TOE is used as a secure application module for the reader/writer device. The TOE includes a secure IC chip with an embedded operating system. The secure IC chip is the AE57C1 developed by Renesas Technology Corporation. This IC chip is certified in CC v2.3 as EAL4 augmented with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

Figure 1 shows the functional configuration of the reader/writer and the TOE.

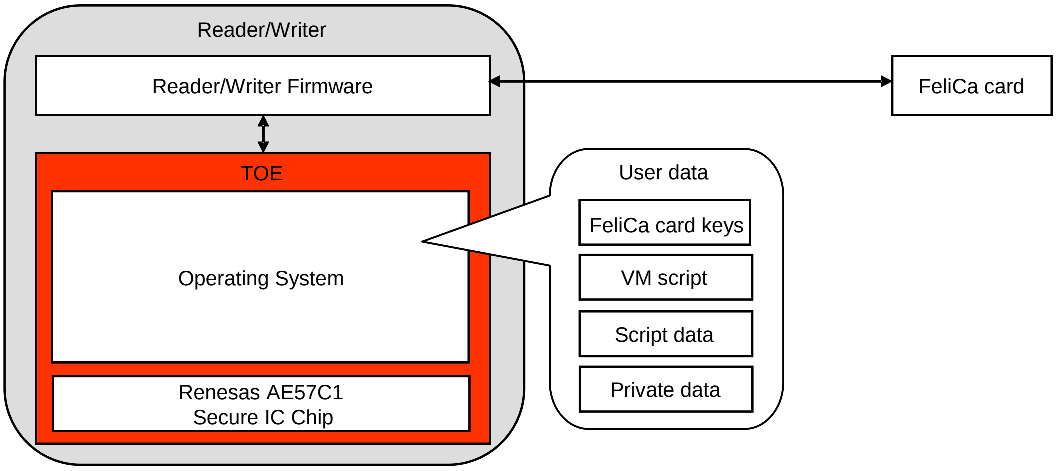

Figure 1: Functional configuration of the reader/writer and the TOE

The main function of the TOE is to encrypt and decrypt packet-based data in accordance with the FeliCa technology. By inserting the TOE into a Subscriber Identity Module (SIM) slot of a reader/writer, the reader/writer can use the functions offered by the TOE through the interface while conforming to the specification of ISO/IEC 7816. Therefore, with the help of the TOE, the reader/writer can communicate with the FeliCa card. For the FeliCa card user, this enables the provision of various services, such as transportation services and financial services.

Security Assurance Requirements

The product was evaluated with all the evidence required to fulfil EAL4, augmented with the components related to the vulnerability analysis AVA_VAN.5 and also for ALC_DVS.2, according to CC Part 3 [CC-P3].

Also the additional activities for composite product evaluation defined by JIL in the document [CPE] were performed by the laboratory and validated by the CB. They are described in the table below as “XXX_COMP.n” components.

Assurance Class	**Assurance Components**
Security Target	ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.2, ASE_ECD.1, ASE_REQ.2, ASE_TSS.1 and ASE_COMP.1
Development	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3 and ADV_COMP.1
Guidance	AGD_OPE.1 and AGD_PRE.1
Life Cycle	ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1 and ALC_COMP.1
Tests	ATE_COV.2, ATE_DPT.2, ATE_FUN.1, ATE_IND.2 and ATE_COMP.1
Vulnerability Analysis	AVA_VAN.5 and AVA_COMP.1

Security Functional Requirements

The product security functionality satisfies several requirements as stated by its Security Target, and according to CC Part 2 [CC-P2]. They are requirements for security functions such as information flow control, identification and authentication.

These functional requirements satisfied by the product are:

FMT_SMR.1	Security roles
FIA_UID.1	Timing of identification
FIA_UAU.1	Timing of authentication
FIA_UAU.4	Single-use authentication mechanisms
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_SMF.1	Specification of Management Functions
FDP_SDI.2	Stored data integrity monitoring and action
FTP_ITC.1	Inter-TSF trusted channel

Identification

Product: RC-S251/SO2 v1.0.

Security Target: Security Target RC-S251/SO2, v1.1, December 2008.

Protection Profile: none.

Evaluation Level: CC v3.1 r2 EAL4+ (AVA_VAN.5, ALC_DVS.2).

Security Policies

The usage of RC-S251/SO2 v1.0 as a composite smartcard product implies to implement a series of organizational policies that assure the commitment of different demands of security.

The details about them are included in the Security Target. In synthesis, the necessity settles down to implement organizational policies relative to:

P.Confidentiality **The TOE shall provide means to protect the confidentiality of the stored assets.**

The TOE shall have some security measures that can protect the stored user data from unauthorized disclosure. We do not expect the TOE to enforce these security measures on any or all user data, but those measures shall be available when the user decides that they shall be used for some of the user data.

P.Integrity **The TOE shall provide means to protect the integrity of the stored assets.**

The integrity of the stored assets shall be protected during operation in a hostile environment. To ensure the integrity, the TOE shall have some security measures that can protect the stored user data from unauthorized modification and destruction.

P.TransferSecret **The TOE shall provide means to protect the confidentiality of assets during transfer from the outside of TOE.**

Should the user decide so, user data that is sent or received through the communication channel needs protection from unauthorized disclosure. The TOE shall provide the capabilities to provide such measures.

P.TransferIntegrity **The TOE shall provide means to protect the integrity of assets during transfer from the outside of TOE.**

The integrity of the messages on the communication channel shall take into account both the possibility of benign interference and malicious interference in various forms, such as: RF noise, spikes in the field, short removals of the field, ghost transmissions, replay, and injection of data into the channel. The TOE shall provide the means to ensure the integrity of user data transferred.

P.Execute **The TOE shall allow only authorized users to execute packet encryption and decryption functions.**

The TOE shall have some security measures to protect the functions that use the stored user data from execution by an unauthorized user. To prevent illegal use, the TOE shall provide only the authorized user with access to the packet encryption and decryption functions, which use the user data.

P.Keys **The keys generated for the use by TOE shall be secure. The keys for the use by TOE shall be generated and handled in a secure manner.**

Some keys are generated for the TOE externally, by the supporting system in a controlled environment. This system shall check that the keys are suitably secure, for example, by weeding out weak keys. Some keys are generated outside the TOE for use by the TOE. These keys are then loaded into the TOE. The process of key generation and management shall be suitably protected and shall occur in a controlled environment.

Assumptions and operational environment

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target, and briefly described below. These same assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

In this TOE ST there is only one assumption to be considered:

A.Process **The TOE is administered in a secure manner after the TOE delivery.**

The customer is responsible for the secure administration of the TOE and protected storage. It is assumed that security procedures are used between delivery of the TOE by the TOE manufacturer and delivery to the customer, to maintain the confidentiality and integrity of the TOE and its manufacturing and test data (to prevent any possible copying, modification, retention, theft for unauthorized use). This means that assets after TOE delivery are assumed to be protected appropriately.

Threats

As described in the ST, the TOE objectives are focused on addressing the previous list of policies. In this case the developer has not included any explicit list of threats in the ST.

Operational environment objectives

The product requires the cooperation from its operational environment to fulfil the requirements listed in its Security Target. This section identifies the IT security objectives that are to be satisfied by the imposing of technical or procedural requirements on the TOE operational environment. These security objectives are assumed by the Security Target to be permanently in place in the TOE environment.

With this purpose, the security objectives declared for the TOE environment are the following:

OE.Keys **The handling of the keys outside the TOE shall be performed in accordance to the specified policies.**

Specific keys for use by the TOE are generated externally (that is, beyond control of the TOE). The generation and control of the keys shall be performed in strict compliance to the specific policies set for such operations.

OE.Process **The handling of the TOE after the TOE delivery shall be performed in a secure manner.**

In the environment of the TOE, confidentiality and integrity of the TOE and its manufacturing and test data shall be maintained by means of procedural measures between delivery of the TOE by the TOE manufacturer and delivery of the TOE to the customer.

TOE Architecture

As previously described in this document, the TOE is a composite smartcard to be used as a SAM (Secure Application Module) for the reader/writer device interacting with a Felica card.

To start communication with the FeliCa card, the Reader/Writer Firmware must mutually authenticate the TOE and then establish the encrypted secure-communication channel with the TOE. Then, to continue the communication after successful authentication, the TOE provides the encryption/decryption function to the authenticated Reader/Writer Firmware. This function enables the Reader/Writer Firmware to encrypt or decrypt packet-based data in accordance with the FeliCa technology. Therefore, the reader/writer can communicate with the FeliCa card and it is possible for the user to provide various services that use the FeliCa card. For executing the encryption or decryption, the TOE allows the registration of FeliCa card keys. To securely execute encryption or decryption, the TOE has security measures that aim to maintain the confidentiality and integrity of FeliCa card keys.

In addition, the TOE allows the registration and execution of Virtual Machine (VM) scripts, so the user of the reader/writer can add bespoke functions to the TOE. VM scripts are used for two distinct purposes, as follows:

- Generate a signature from supplied input information.
  The signature algorithm runs on the VM on the TOE.
- Generate a unique value based on a proprietary individualization algorithm.
  This value is used during mutual authentication with the FeliCa card. The individualization algorithm runs on the VM on the TOE.

These algorithms are implemented by VM scripts. The TOE also allows registration of Script data and Private data, which is necessary to execute the signature algorithm and individualization algorithm with VM scripts. To register and execute VM scripts, Script data and Private data securely, the TOE has security measures that aim to maintain the confidentiality and integrity of VM scripts, Script data and Private data.

The TOE has several self-protection mechanisms to satisfy all requirements for self-protection, non-bypassability and domain separation for the smartcard security.

The physical architecture of the TOE and its operational environment is illustrated by figure 1. In this figure we can see:

- The ***boundary*** of the TOE is indicated in red. The form factor of the TOE is the ID-1/000 card. The ID-1/000 card is specified in ISO 7810. It is an ID-1 size card containing an ID-000-size card. Its physical characteristics are specified in ISO 7810.

- **“Operating System”** is the part of the TOE that is responsible for executing both the processing related to the VM scripts and the packet encryption/decryption for communication with the FeliCa card. It has security measures that aim to maintain the confidentiality and integrity of FeliCa card keys, VM scripts, Script data and Private data.
- **“Renesas AE57C1”** is the hardware platform (the IC) and is part of the TOE. It has detectors, sensors, and circuitry to protect the TOE.
- **“Reader/Writer Firmware”** is responsible for execution of both the reader/writer application and the packet control that conforms to the ISO 7816 and ISO 18092. “Reader/Writer Firmware” is out of scope of the TOE.
- **“FeliCa card”** is an external contactless IC card that conforms to the ISO 18092. “FeliCa card” is out of scope of the TOE.

Documents

The basic documentation distributed with the TOE to be used with the security assurance provided by the certificate issued is:

- *RC-S251 Command interface manual, v1.0*
- *RC-S251 Rewriting Transport Key (Maintenance mode), v1.01*
- *RC-S251 Rewriting Transport Key (Admin/Normal mode), v1.01*
- *RC-S251 Important Requirements for an Operation, v1.0*
- *RC-S251 Management Tool Reference Manual, v1.01*

TOE Testing

The manufacturer has developed testing for the TOE TSF. All these tests have been performed by the manufacturer in their location and facilities with success.

The process has verified each unit test, checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target.

It is been checked also that the obtained results during the tests fit or correspond to the previously estimated results.

The evaluator examined the design specification and test documentation, concluding that all the modules functionality (low level design) are tested. Therefore, all TSFIs are fully tested. The evaluator verified that TSFI were tested in test plan. The test procedures mapped all TSFI to SFR-enforcing modules.

The evaluator has repeated all the tests defined in the TOE test specification according to the different configurations defined the developer. All tests have been successfully performed.

The developer provides all the equipment necessary to perform independent testing, as shown in the following list:

– TOE in form factor ID-1/000
– ™Renesas Hardware Emulator (E6000H).
– 1 contact smart card reader to attach the Emulator
– 5 FeliCa pasori USB readers (RC-S320), all containing a FeliCa test card.
– One FeliCa serial reader (RC-S440), with a FeliCa test card.
– All software required to create test environment

The evaluator executed the tests and updated the test documentation with new devised tests. The evaluator verified that the obtained results were agreed with expected results. The tests where organized around the functionality of:

- Secure storage of user data
- Secure transfer of user data
- Secure management of user data

Evaluator chose the tests with a selection criteria based on:

– Selection of all developers test customised to be executed on the real TOE.
– Testing the security storage with specialists equipment to simulate external factors (glitching) to check the feasibility of the CRC counter measure not the consequence of being implemented.
– Testing the secure transfer based on T=1 implementation over a real environment.
– Validate the correctness of sequence identifier, cipher and MAC.
– Finally, complement testing with random techniques (fuzzing over available commands) over the secure management TSF.

The result of independent tests was successfully performed and there were neither inconsistencies nor deviations between the actual and the expected results.

Penetration Testing

The evaluator defined as research criterion to identify potential vulnerabilities the use of the JIL Attack Methods reference [AMS] and the Renesas IC ETR-lite for the composition, complemented with:

- Specialist publication in terms of secure coding in C and assembler
- Use of CHES proceedings
- Use of Cryptoanalysis specialist proceedings

The evaluator devised the a methodology to perform methodical vulnerability assessment analysis based in two phases:

– A bottom-up strategy analyses the source code to detect software bugs or flaws. To confirm the existence of bug or flaw the high level evidences must be used.

– A top-down strategy analyses the high level design taking into account the security architecture to formulate flaw hypothesis. To confirm the flaw hypothesis the low level evidences must be used.

To confirm the completeness of the methodology the whole source code, the whole top level (subsystem and modules) design and the security architecture should be analysed.

The independent penetration testing devised several test cases covering the main types of attacks in [AMS] including physical attacks, probing, overcoming of sensors and filters, clock and voltage glitches, DFA, perturbation and light attacks (laser), SPA/DPA, EMA, EEPROM attacks, and software attacks.

The evaluator did not find neither exploitable vulnerabilities nor residual vulnerabilities in the operational environment as a result of independent penetration testing.

Evaluated Configuration

The TOE is defined by its name and version number **RC-S251/SO2 v1.0**.

The source code is the **r1203**.

The form factor the **ID-1/000 card**. The ID-1/000 card is an ID-1 size card containing an ID-000-size card.

Evaluation Results

The composite product RC-S251/SO2 v1.0 on the integrated circuit for intelligent card Renesas AE57C1 has been evaluated in front of the “Security Target RC-S251/SO2”, v1.1, December 2008.

All the assurance components required by the level EAL4+ (augmented with AVA_VAN.5, ALC_DVS.2) have been assigned a “PASS” verdict. Consequently, the laboratory (LGAI-APPLUS) assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4 methodology, as define by of the Common Criteria [CC-P3] and the Common Methodology [CEM].

Comments & Recommendations from the Evaluation Team

The developer follows all the underlying platform security recommendations and contributes with additional countermeasures to enforce the security of the whole product. Therefore the RC-S251/SO2 v1.0 fulfils the requirements of CC version 3.1 with an evaluation assurance level EAL4+ augmented with ALC_DVS.2 and AVA_VAN.5.

To identify the TOE version check the "Command Interface Manual" for the command about how to get the information of the chip.

Certifier Recommendations

Considering the obtained evidences during the instruction of the certification request of the RC-S251/SO2 v1.0 composite product on the integrated circuit for intelligent card Renesas AE57C1, a positive resolution is proposed.

Note that this composite TOE claim for CC v3.1 EAL4+ with ALC_DVS.2 and AVA_VAN.5, and the IC platform level of assurance is CC v2.3 EAL4+ with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

The certification body authorised the evaluation although the CC versions were different, based on:

- EAL4 for v2.3 is equivalent to EAL4 for v3.1.
- ALC_DVS.2 is one assurance requirement of both.
- AVA_VAN.5 is considered equivalent to AVA_MSU.3 and AVA_VLA.4.

Therefore the EAL chosen for the composite evaluation does not exceed the EAL applied to the evaluation of the platform.

Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

Acronyms

APDU Application Protocol Data Unit

CB Certification Body

CC Common Criteria

COT Chip on Tape

EAL Evaluation Assurance Level

EEPROM Electronically Erasable Programmable Read Only Memory

EMA ElectroMagnetic Analysis

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functionality

PP Protection Profile

RNG Random Number Generator

SAR Security Assurance Requirement

SFR Security Function Requirement

SIM Suscriber Identity Module

SPA/DPA Simple/Differential Power Analysis

VM Virtual Machine

Bibliography

The following standards and documents have been used for the evaluation of the product:

Common Criteria

[CC_P1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, Version 3.1, r1, September 2006.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, r2, September 2007.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, r2, September 2007.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 3.1, r2, September 2007.

JIL papers

[AAP] Application of Attack Potential to Smartcards v2.7

[CPE] Composite product evaluation for Smart Cards and similar devices v1.0

[SCG] Smartcard evaluation guidance v1.2

[ARC] Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices v1.0 (trial)

[CDE] Collection of Developer Evidence v1.1

[AMS] Attack Methods for Smartcards and Similar Devices v1.5

[RIC] Requirements to perform Integrated Circuit Evaluations v1.0

Security Target

It is published jointly with this certification report the security target,

“Security Target RC-S251/SO2”, v1.1, December 2008.

Public version: “Security Target RC-S251/SO2”, v1.1, July 2009..