Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0590-2009

for

IC chip for the reader / writer RC-S940 (CXD9768GG), Version 4

from

Sony Corporation

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0590-2009

IC chip for the reader / writer
RC-S940 (CXD9768GG), Version 4

from	Sony Corporation
PP Conformance:	None
Functionality:	product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 4

Common Criteria
Recognition
Arrangement

Common Criteria

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, Part 1 Version 0.6, Part 2 Version 1.0 extended by advice of the Certification Body for smart card specific guidance for conformance to the Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999) and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

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 certification scheme of the German Federal Office for Information Security (BSI) 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 the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 30 July 2009
For the Federal Office for Information Security

IT Security Certified
SOGIS - MRA

Irmela Ruhrmann
Head of Division

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.1 [1]
- Common Methodology for IT Security Evaluation (CEM) [2]
  - Part 1, Version 0.6
  - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

The use of Common Criteria Version 2.1, Common Methodology, part 2, Version 1.0 and final interpretations as part of AIS 32 results in compliance of the certification results with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2 as endorsed by the Common Criteria recognition arrangement committees.

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became initially effective in March 1998.

This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and United Kingdom, and from The Netherlands since January 2009 within the terms of this agreement.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of January 2009 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product IC chip for the reader / writer RC-S940 (CXD9768GG), Version 4 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0308-2005. Specific results from the evaluation process BSI-DSZ-CC-0308-2005 were re-used.

The evaluation of the product IC chip for the reader / writer RC-S940 (CXD9768GG), Version 4 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 19 May 2009. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Sony Corporation

The product was developed by: Sony Corporation

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

[5] Information Technology Security Evaluation Facility

4 Validity of the certification result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report and in the Security Target.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product IC chip for the reader / writer RC-S940 (CXD9768GG), Version 4 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http://www.bsi.bund.de) and [5]. Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Sony Corporation
Gate City Osaki, Osaki East Tec.
1-11-1 Osaki Shinagawa-ku, Tokyo
141-0032 Japan

This page is intentionally left blank.

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Executive Summary

The Target of Evaluation (TOE) is an IC-Chip with the product name “RC-S940” (product code ”CXD9768GG”, produced at the Oita wafer production site[7]) Version 4 that will be embedded into a Smart Card Reader/Writer. The IC chip (refer to Figure 1: Block Diagram of TOE) consists of memories (16kBytes ROM, 128kBytes EEPROM, and 4kBytes SRAM), data bus, security logic, peripheral devices, I/O interface, a dedicated CPU, etc. In ROM the program for control to the IC chip is stored; in EEPROM authentication data and a downloadable firmware (which is out of scope of the TOE) are stored; in SRAM area communication data and other processed data are stored as temporary data. The TOE contains some security logic (Random Number Generator, CRYPTO Engine and Illegal Voltage/Frequency/Temperature Detection Sensors) and peripheral devices (Timer, Interrupt Controller, Clock Gear and Reset Generator) are used for maintaining performance and security. The IC-Chip provides an UART interface used for communication with the controller (e.g. a PC connected to the Reader/Writer the TOE is built in) and a RF CARD interface used for communication with a contactless Smart Card (RF CARD interface and an other inactivated circuit is out of scope of the TOE).
This IC-Chip provides different operating modes. IPL (Initial Program Load) Mode and STOP Mode are within the scope of this evaluation. Normal Mode (i.e. running a firmware, which was downloaded in IPL Mode) is out of scope in this evaluation.

The IC-Chip provides the security functionality of mutual authentication and subsequent secure download of some application firmware (which is out of scope of the TOE) to EEPROM used for activation of the external communication interface in Normal mode (this interface and Normal mode are out of scope of the TOE). Furthermore, the TOE provides physical and logical security functionality to prevent disclosing or modification of data stored inside the IC-Chip. The concrete security functions of the TOE are listed in table 1.

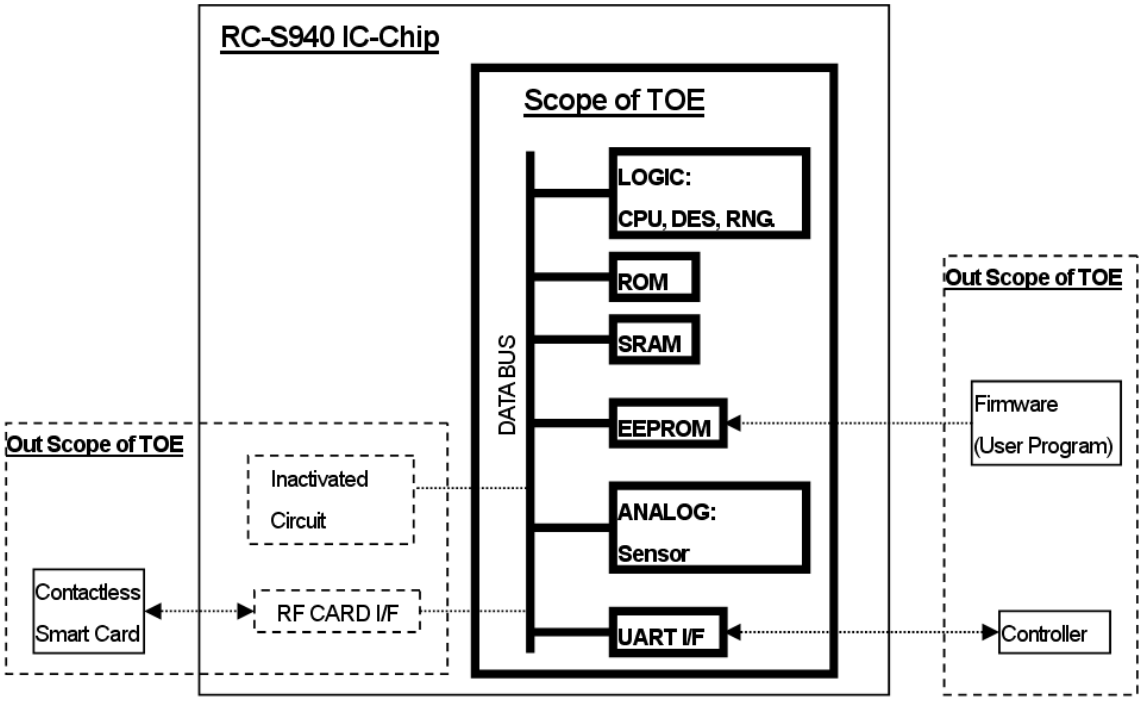

Figure 1: Block diagram of the RC-S940

[7] Sony confirms that the RC-S940 will be produced only at the Oita wafer production site, which was part of the evaluation.

Configuration of the functional blocks of TOE is as listed below:

- CPU: TLCS-900/L1 CPU is a 16-bit CPU. It has 16Mbytes of linear address space.
- SRAM: 4kB SRAM built in the IC-Chip.
- ROM: 16kB ROM built in the IC-Chip.
- ROM program stored in the ROM.
- EEPROM: 128kB (64kB x 2) EEPROM built in the IC-Chip.
- A part of data (cryptographic keys) stored in the EEPROM.
- Firmware (out of scope of the TOE) stored in the EEPROM.
- Security Logic: The security logic contains a cipher co-processor (Triple DES, compatible with ECB Mode / CBC Mode), random number generation function, and detect function (illegal voltage detect function, illegal frequency detect function, illegal temperature detect function).
- Peripheral Equipment: Peripheral equipment contains a 16-bit timer, interrupt controller, reset controller, and clock gear.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the Assurance Requirements of the Evaluation Assurance Level EAL 4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 5.1.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6] and [9], chapter 5.2.

The TOE Security Functional Requirements are implemented by the following TOE Security Functions:

TOE Security Function	Addressed issue
SF.1	Detection of illegal operation
SF.2	Protection to information leakage
SF.3	Physical protection
SF.4	Encryption of data
SF.5	Mutual authentication
SF.6	Protection of data passing through the interface
SF.7	Self Test
SF.8	Protection of internal data

Table 1: TOE Security Functions

For more details please refer to the Security Target [6] and [9], chapter 6.1.

The claimed TOE's Strength of Functions 'basic' (SOF-basic) for specific functions as indicated in the Security Target [6] and [9], chapter 6.1 is confirmed. The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 3.1 . Based on these assets the TOE Security Environment is defined in terms of Assumptions and Threats. This is outlined in the Security Target [6] and [9], chapter 3.2 and 3.3.

This certification covers the following configurations of the TOE: The Security Target [6] and [9] identifies only one configuration of the TOE, the IC chip for the reader / writer RC-S940 (CXD9768GG), version 4. For details please refer to chapter 8.

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

IC chip for the reader / writer
RC-S940 (CXD9768GG), Version 4

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW / FW	IC chip *RC-S940* (product code *CXD9768GG produced at the Oita wafer production site*), i.e. the TOE (including ROM Program version 3, Mask set version 3)	4	Trusted carrier and sealed packaging
2	DOC	Document *RC-S940 IPL Users Manual [10]*	1.0	Electronic transfer, PGP-encrypted
3	DOC	Document *RC-S940 Operation Guideline [11]*	1.1	Electronic transfer, PGP-encrypted
4	DOC	Document *RC-S940 Administrator Tools Manual [12]*	2.0	Electronic transfer, PGP-encrypted
5	DOC	Shipping key and program signature	N/A	Electronic transfer, PGP-encrypted
6	DOC	Correspondence table: serial no. vs. ID number IDm	N/A	Electronic transfer, PGP-encrypted

Table 2: Deliverables of the TOE

3 Security Policy

The security policy of the TOE is to provide security functionality for a secure download of firmware to the EEPROM and for secure communication between the controller and the IC-Chip.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies 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: Secure communication channel, management of external TOE data, personnel and delivery procedures. Details can be found in the Security Target [6] and [9] chapter 4.2.

5 Architectural Information

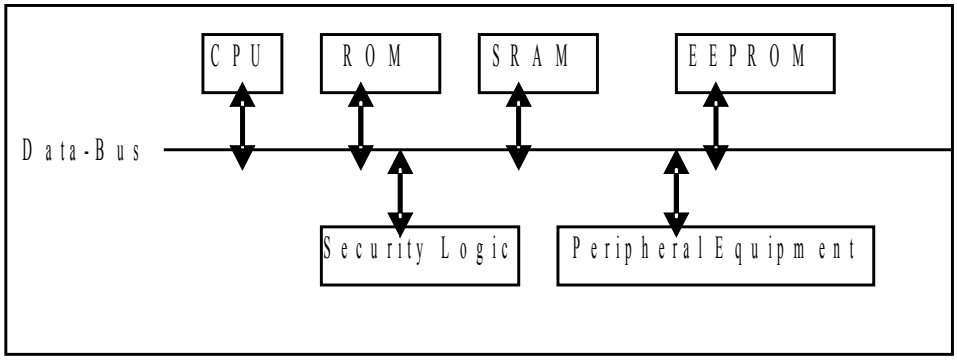

Figure 2: Block diagram of TOE

The configuration of the functional blocks of the TOE are:

- CPU: 16bit CPU with 16Mbytes of linear address space.
- SRAM: 4kB SRAM built in the IC-Chip.
- ROM: 16kB ROM built in the IC-Chip.
- ROM program stored in the ROM.
- EEPROM: 128kB (64kB x 2) EEPROM built in the IC-Chip.
- A part of data (cryptographic key) stored in the EEPROM.
- Firmware (out of scope of the TOE) stored in the EEPROM.
- Security Logic: The security logic contains a cipher co-processor (Triple DES), random number generation function, and detect function (illegal voltage detect function, illegal frequency detect function, illegal temperature detect function).
- Peripheral Equipment: Peripheral equipment contains a timer, interrupt controller, reset controller, and clock gear.

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

7.1 Developer's Test according to ATE_FUN

The developers testing effort can be summarized in the following four aspects.

TOE test configuration:

- The tests are performed with the chip RC-S940 Version 4. To be able to test all TSF in detail some tests special prepared chips are used.

Testing approach:

- All TSF and related sub-functions and subsystems are tested in order to assure complete coverage of all SFR, addressing both hardware and ROM program functionalities of the TOE. The developer combines automated test tools and manual test procedures, as appropriate for the item under test.

Testing depth:

- The tests are performed on (sub-) function level and can be mapped to mechanisms interfaces and sub systems.
- The developer has tested the TOE systematically at the level of TSF functionalities as given in the functional specification.
- The developer has tested the TOE systematically at the level of the subsystems as given in the high level design.
- The entire test set comprises 756 individual test cases.

Testing result:

- All testing strategies of the TSF passed all tests of individual tests.
- Overall the TSF have been tested systematically against the functional specification and the high-level design.
- The developer tests demonstrate that the security functions perform as specified.

All test results are as expected and no test failed.

For re-evaluation:

The developer did not repeat any developer testing, as the TOE is unchanged.

7.2 Evaluator Tests

Independent Testing according to ATE_IND:

The independent testing was partly performed in the developer's testing environment in Tokyo, Japan and partly at TNO in Delft, Netherlands. During the testing at the developer's site the same platforms and tools as for the developer tests were used.

The evaluator's objective regarding this aspect was to test the functionality of the TOE as described in functional specification and the high level design, and to verify the developer's test results by sampling a representative set from the developer's tests and additionally add independent tests.

The results of the specified and conducted independent evaluator tests confirm the TOE functionality as described in functional specification and the high level design. The TOE security functions were found to behave as specified.

The results of the developer tests, which have been repeated by the evaluator, matched the results the developer stated in the developer test documentation.

For re-evaluation:

The evaluator did not repeat any developer testing, as the TOE is unchanged.

Penetration Testing according to AVA_VLA:

The penetration testing was performed by the subcontracted hardware evaluation facility of TNO. Due to the nature of this testing, specific hardware investigation and electronic lab equipment was used.

For re-evaluation:

As result of the Summary Report Theoretical Vulnerability Analysis the evaluator conducted Evaluation Body Testing.

The conducted penetration testing confirms that the TOE in the intended environment of use does not feature any exploitable vulnerability for attackers with low attack potential.

8 Evaluated Configuration

This certification covers the following configurations of the TOE: The Security Target [6] and [9] identifies only one configuration of the TOE. The tests are performed with the chip RC-S940. This is in consistence to the configuration identified in the Security Target [6] and [9].

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used.

The following guidance specific for the technology was used:

(i) Functionality classes and evaluation methodology for deterministic random number generators

(ii) The Application of CC to Integrated Circuits

(iii) Application of Attack Potential to Smartcards

(see [4], AIS 20, AIS 25, AIS 26) were used.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the class ASE
- All components of the EAL 4 package as defined in the CC (see also part C of this report)

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0308-2005, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on two sites that have moved since the last certification, an update of the vulnerability analysis and additional penetration tests.

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: product specific Security Target
  Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4
- The following TOE Security Functions fulfil the claimed Strength of Function : basic
  - SF1: Detection of illegal operation
  - SF3: Physical protection
  - SF4-1, SF4-3: Pseudo Random Number Generator part
  - SF5: Mutual authentication
  - SF6: Protection of data passing through the interface

In order to assess the Strength of Function the scheme interpretations AIS 20, AIS 25 and AIS 26 (see [4]) were used.

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This holds for:

- the TOE Security Function SF4-2 (Triple DES Cipher system).

10 Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Security Target

For the purpose of publishing, the Security Target [9] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12 Definitions

12.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Errichtungsgesetz
CBC	Cipher Block Chaining
CC	Common Criteria for IT Security Evaluation
CCRA	Common Criteria Recognition Arrangement
DES	Data Encryption Standard; symmetric block cipher algorithm
EAL	Evaluation Assurance Level
ECB	Electrical Code Block
EEPROM	Electrically Erasable Programmable Read Only Memory
ETR	Evaluation Technical Report
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
RAM	Random Access Memory
ROM	Read Only Memory
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

12.2 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.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

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

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

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.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

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

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.[8]

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Website

[6] Security Target BSI-DSZ-0308-2005, Version 2.04, 13 May 2005, RC-S940 Security Target (confidential document)

[7] Evaluation Technical Report, Version 1, Date: 15.04.2009, Product: RC-S940 Version 4 Reader/Writer IC, Evaluation Body for IT-Security of TÜV Informations-technik GmbH (confidential document)

[8] RC-S940 Configuration List, Version 4.6, 27. November 2008, Sony Corporation (confidential document)

[9] Security Target (Public Version) BSI-DSZ-0308-2005, Version 2.04, 13 May 2005, RC-S940 Security Target (sanitised public document)

[10] RC-S940 IPL Users Manual Version 1.0 , 4 March 2004, Sony Corporation

[11] RC-S940 Operation Guideline, Version 1.1, May 26, 2004

[12] RC-S940 Administrator Tools Manual, Version 2.0, June 21, 2005

[8] specifically

- AIS 20, Version 1, 2 December 1999, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 3, 6 August 2007, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 3, 6 August 2007, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

- **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
- **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

- **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.

Assurance Class	Assurance Family
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

Assurance Class	Assurance Family
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 11.1)

“Table 6 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 7 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 11.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 11.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 11.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.”

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.”

“Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”

This page is intentionally left blank.

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0590-2009

Evaluation results regarding development and production environment

The IT product IC chip for the reader / writer RC-S940 (CXD9768GG), Version 4 (Target of Evaluation, TOE) has been evaluated at an accredited and licensed / approved evaluation facility using the Common Methodology for IT Security Evaluation, Part 1 Version 0.6, Part 2 Version 1.0 extended by advice of the Certification Body for smart card specific guidance for conformance to the Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999) and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

As a result of the TOE certification, dated 30 July 2009, the following results regarding the development and production environment apply. The Common Criteria Security Assurance Requirements

- ACM – Configuration management (i.e. ACM_AUT.1, ACM_CAP.4, ACM_SCP.2),
- ADO – Delivery and operation (i.e. ADO_DEL.2, ADO_IGS.1) and
- ALC – Life cycle support (i.e. ALC_DVS.1, ALC_LCD.1, ALC_TAT.1),

are fulfilled for the development and production sites of the TOE listed below:

a) FeliCa Business Division, Sony Corporation (GCO Site)
Role: Development of hardware / ROM Program
Gate City Osaki East Tower, 22F, 1-11-1 Osaki Shinagawa-ku, Tokyo, 141-0032, Japan

b) Ofuna Development Center, Toshiba Corporation (Ofuna Site)
Role: Development of hardware, design of masks
2-5-1, Kasama-cho, Sakae-ku, Yokohama-city, Kanagawa-pref., Japan

c) Oita Factory, Toshiba Corporation (Oita Site)
Role: Manufacture of wafers
3500, Matsuoka, Oita-city Oita-pref., Japan

d) Toshiba LSI Package Solutions Corporation (Kituki Site)
Role: Manufacture of LSI
2820-2, Minami-Kituki, Kituki-city, Oita-pref., Japan

e) Sony EMCS Senmaya Tec (Senmaya Site)
Role: Initialization of the LSI / Installation of the customer's information to the LSI
5254, Shimokomaba,Senmaya Senmaya-cho Ichinoseki-shi, Iwate-pref., Japan

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the Threats, Security Objectives and Requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [9]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.