Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0308-2005

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 +49 228 9582-0, Fax +49 228 9582-455, Infoline +49 228 9582-111

Deutsches
IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0308-2005

IC chip for the reader / writer

RC-S940 (CXD9768GG), version 4

from

Sony Corporation

Common Criteria Arrangement

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.

Evaluation Results:

Functionality:	**product specific Security Target** **Common Criteria Part 2 conformant**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL4**

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.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 01. September 2005

The Vice President of the Federal Office
for Information Security

Hange L.S

IT Security Certified

SOGIS-MRA

.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-455 - Infoline +49 228 9582-111

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)

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)
- Common Criteria for IT Security Evaluation (CC), Version 2.1
- Common Methodology for IT Security Evaluation (CEM)
  - Part 1, Version 0.6
  - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)

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] 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 7 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 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.

2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland, France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003, the Czech Republic in September 2004, the Republic of Singapore in March 2005, India in April 2005.

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, (ROM version 3, Mask set version 3) has undergone the certification procedure at BSI.

The evaluation of the product IC chip for the reader / writer RC-S940 (CXD9768GG), version 4, (ROM version 3, Mask set version 3) was conducted by TUV Informationstechnik GmbH. TUV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by BSI.

The sponsor, vendor and distributor is:

Sony Corporation
4-7-35 Kitashinagawa shinagawa-ku
Tokyo 140-0001, Japan

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 01. September 2005.

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.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

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.

[5] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-20 and D1 to D-4. The product IC chip for the reader / writer RC-S940 (CXD9768GG), version 4, (ROM version 3, Mask set version 3) has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the vendor[6] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[6] Sony Corporation
4-7-35 Kitashinagawa shinagawa-ku
Tokyo 140-0001, Japan

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.

Contents of the certification results

1 Executive Summary

The 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 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 inactivatedcircuit 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 scope of the TOE) to EEPROM used for activation of the external communication interface in Normal mode (this interface and Normal mode are out 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.

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

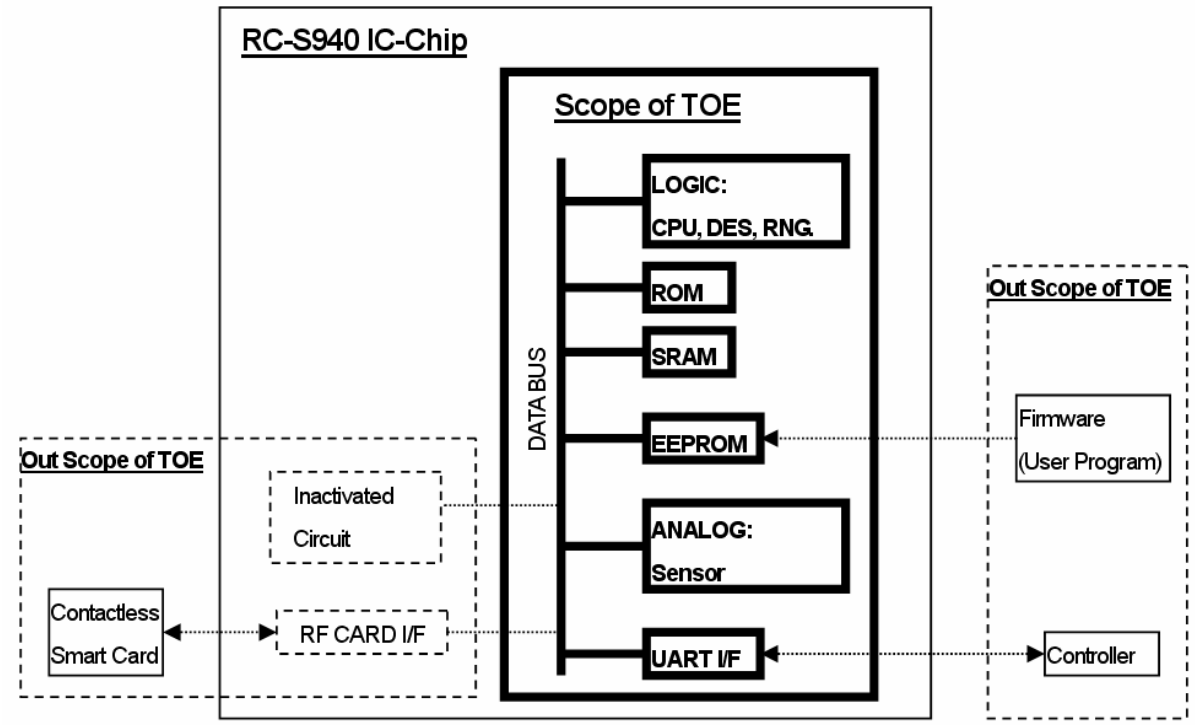

Figure 1: Block diagram of the RC-S940

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 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 IT product was evaluated by TUV Informationstechnik GmbH. The evaluation was completed on 05.07.2005. The TUV Informationstechnik GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor, vendor and distributor is

Sony Corporation
4-7-35 Kitashinagawa shinagawa-ku
Tokyo 140-0001, Japan

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL4 (Evaluation Assurance Level 4).

1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 conformant as shown in the following tables.

The following SFRs are taken from CC part 2:

Security Functional Requirement	**Identifier**
FPT	Protection of the TOE Security Functions
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.3	Resistance to physical attack
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_RCV.4	Function recovery
FPT_TST.1	TSF testing
FDP	User Data Protection
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attribute
FDP_ITT.1	Basic internal transfer protection

[8] Information Technology Security Evaluation Facility

FDP_SDI.1	Stored data integrity monitoring
FDP_UIT.1	Data exchange integrity
FDP_UCT.1	Basic data exchange confidentiality
FCS	Cryptographic Support
FCS_COP.1	Cryptographic operation
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FTP	Trusted Path/Channels
FTP_ITC.1	Inter-TSF trusted channel
FIA	Identification and Authentication
FIA_UID.1	Timing of identification
FIA_UAU.2	User authentication before any action
FIA_AFL.1	Authentication failure handling
FMT	Security Management
FMT_SMR.1	Security roles
FMT_MTD.1	Management of TSF data
FMT_MSA.2	Secure security attribute
FMT_MSA.3	Static attribute initialization
FMT_MSA.1.A	Management of security attributes
FMT_MSA.1.B	Management of security attributes
FIA_SMF.1	Specification of Management Functions

Table 1: SFRs CC part 2 extended

Note: Only the titles of the Security Functional Requirements are provided. For more details please refer to the Security Target (Public Version) [7], chapter 5.

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

TOE Security Functions	**Description**
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 2: TOE Security Functions

SF.1: Detection of illegal operation

This function detects illegal temperature, voltage, and frequency of TOE that outside the normal operating scope of TOE because of trouble, accident, or intentional act during data processing by TOE.

When detected any abnormal values, the TOE performs a system reset.

Security functional requirements satisfied: FPT_PHP.3, FPT_FLS.1, FPT_RCV.4.

SF.2: Protection to information leakage

To convert the information leaked out of hidden channels located within TOE during encryption process and computation process into non-beneficial information, the SPA/DPA-resistant CRYPTO Engine is used as the countermeasures against power consumption analysis to provide protection to the confidentiality of data during encryption process and computation process.

Security functional requirements satisfied: FDP_IFC.1, FDP_IFF.1, FDP_ITT.1, FPT_ITT.1.

SF.3: Physical protection

A special TOE design and construction (“Tamper Resistant Layout” which uses glue logic layout, shield layers, etc.) makes physical analysis (reverse engineering) or modification (tampering) of the TOE difficult.

In addition entry into Test Mode is protected by different protection functions.

These features protect the integrity of the complete TOE including SRAM, ROM, and EEPROM.

It therefore protects all User and TSF Data against disclosure by physical probing when stored or while being processed by the TOE.

SF.3 supports the correct and secure operation of all other security functions and is effective in all operational modes permitted after TOE delivery.

Security functional requirements satisfied: FPT_PHP.3

SF.4: Encryption of data

To perform the encryption of communication data, "CRYPTO Engine" and "Pseudorandom Number Generator" provide support to the encryption as well as the generation of pseudo random numbers.

Note: The functionality of SF4 (Pseudo random number generation and DES engine) described in the following is limited to the operation of the TOE in IPL mode.

SF.4-1: CRYPTO Engine

CRYPTO Engine performs encryption / decryption processes of communication data using the pseudo random numbers generated by Pseudorandom Number Generator.

Generation of this pseudo random number conforms to the following standards.

- “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications” (except 2.6 Discrete Fourier Transform (Spectral) Test), NIST Special Publication 800-22 (with revisions dated May 15,2001).
- "Application Notes and Interpretation of the Scheme (AIS), Functionality classes and evaluation methodology for deterministic random number generators”, AIS 20, Version 1 as of 1999-12-02.

SF4-2: Cipher system supported

Triple DES Cipher system

For the mutual authentication in IPL mode between TOE and the controller, a secure communication is achieved using Triple DES cipher system in which a 112-bit key is used.

Secure communication in IPL mode between TOE and the controller is achieved using Triple DES cipher system. The mode of operation is CBC mode.

SF4-3: Processes supported

The pseudo random number is used for encryption / decryption processes of the communication data and as the data for noise generation as the countermeasures against DPA.

Security functional requirements satisfied: FCS_CKM.1, FCS_COP.1

SF.5: Mutual authentication

This is the authentication function for prevention of illegal access.

SF5-1: IPL mutual authentication

IPL mutual authentication is performed between the controller and TOE when the administrator who knows IPL authentication key executed IPL mutual authentication from the terminal to which the controller is connected.

During IPL mutual authentication, the confidentiality of communication data on the interface is protected by Triple DES cipher system. This is also true for the case of communication data after successful IPL mutual authentication.

SF 5-2: IPL Lock Function

In this IPL mode, IPL Lock function is activated to prevent illegal data access by spoofing an administrator during IPL mode. If IPL mutual authentication successively failed, this function locks the system and after that, execution of IPL mutual authentication is impossible.

Allowable limit of successive failures of IPL mutual authentication is set up at the time of shipping of TOE.

Security functional requirements satisfied: FIA_UID.1, FIA_UAU.2, FIA_ALF.1, FDP_ACC.1, FDP_ACF.1, FMT_SMR.1, FMT_MTD.1, FMT_MSA.1.A, FMT_MSA.1.B, FMT_MSA.2, FMT_MSA.3, FMT_SMF.1., FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FTP_ITC.1

SF.6: Protection of data passing through the interface

External interface used: UART I/F

Communication in IPL mode

Communication data during IPL mutual authentication is protected by Triple DES cipher system.

Communication data after successful IPL mutual authentication is also protected by Triple DES cipher system.

Parity check is used for checking the communication data packet.

Checksum is used for checking the communication data.

Security functional requirements satisfied: FCS_COP.1, FDP_SDI.1, FTP_ITC.1, FDP_UIT.1, FDP_UCT.1, FPT_FLS.1, FPT_RCV.4, FDP_IFC.1, FDP_IFF.1.

SF.7 Self Test

At the initial start-up of the TOE, performs self-test on pseudo-random number generation.

At the initial start-up of the TOE, performs self-test on encryption / decryption functions.

At the initial start-up of the TOE, performs CRC check to the ROM.

At the initial start-up of the TOE, performs Checksum test or CRC check to EEPROM.

At the initial start-up of the TOE, performs CRC check to EEPROM if the firmware is downloaded in EEPROM of TOE.

Security functional requirements satisfied: FPT_TST.1, FDP_SDI.1, FPT_FLS.1, FPT_RCV.4.

SF.8 Protection of internal data

Even if the data being written to EEPROM during loading firmware is corrupted, "Double Buffering" protects the integrity of written data. Double Buffering detects the corrupted data, and restores the data to the state before data writing, i.e. when loading firmware to one buffer fails, still the previously loaded firmware in the other buffer will be active.

By setting "One Time Write" function to "Enable" state, it is possible to inhibit illegal data write to EEPROM to protect parameters that define the behaviour of the security functions from being modified any further. At the time of data write to EEPROM, in addition, "Verify" process is performed.

Security functional requirements satisfied: FDP_SDI.1, FPT_FLS.1, FPT_RCV.4.

1.3 Strength of Function

The TOE's strength of functions is claimed SOF-basic for specific functions as indicated in the Security Target (Public Version) [7], chapter 5. 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) (see Chapter 9 of this report). For rating of SF4-1 and SF4-3 the corresponding requirements from AIS20, "Functionality classes and evaluation methodology for deterministic random number generators", Version 1, 1999-12-02, will be applied with a target of Functionality Class K2 and strength of mechanism medium according to AIS20.

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

There are no Organisational Security Policies addressed by the evaluated IT-product. The threats which were assumed for the evaluation and averted by the TOE are specified in the Security Target (Public Version) [7], divided in three sections:

Threads to IC-Chip

- Malfunction due to Environmental Stress
- Forced Information Leakage

- Inherent Information Leakage
- Physical Probing
- Physical Manipulation
- Cloning

Threats to ROM Program

- Invalid Access
- Monitoring Data
- Power Down

Threats assumed to environment

- Attacks during delivery

1.5 Special configuration requirements

The RC-S940 has four operational modes, Normal Mode, IPL Mode, STOP Mode and TEST Mode.

The Normal Mode allows normal communication with the controller and/or card, which is executed by firmware stored to EEPROM. Normal Mode ist out of scope of the TOE.

The Test Mode is used in manufacturing process. The Test Mode is prohibited after TOE delivery.

The IPL Mode is used to download firmware from the controller to RC-S940. In this mode, communication interface with the card is deactivated.

The STOP Mode is entered automatically when, for example, the internal EEPROM data is damaged. The STOP Mode prevents the RC-S940 from being used under abnormal conditions. All commands except maintenance command cannot therefore be executed.

There are no special security measures for the startup of the TOE besides the requirement that the controller has to be used under the well-defined operating conditions.

1.6 Assumptions about the operating environment

It is assumed that

- the management of external TOE data is performed in a secure manner
- the IC designer / developer, IC manufacturer, delivery personal, Administrator, and firmware developer are trustworthy
- the Controller is capable to establish a secure communication channel

1.7 Disclaimers

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

Deliverable	Version	Medium	Protection
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	Hardware	Trusted carrier and sealed packaging
Document *RC-S940 IPL Users Manual*	1.0	Electronic transfer	PGP-encrypted
Document *RC-S940 Operation Guideline*	1.1	Electronic transfer	PGP-encrypted
Document *RC-S940 Administrator Tools Manual*	2.0	Electronic transfer	PGP-encrypted
Shipping key and program signature	N/A	Electronic transfer	PGP-encrypted
Correspondence table: serial no. vs. ID number IDm	N/A	Electronic transfer	PGP-encrypted

Table 3 Deliverables to customer

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

4.1 Assumptions

The following assumptions are described in the Security Target (Public Version) [7]:

- It is assumed that the management of external TOE data is performed in a secure manner.
- It is assumed that IC designers, IC developers, IC manufacturers, IC delivery personal, Administrator, and firmware developer who are privileged to operate and to manage the TOE are trained about operate and management of TOE, do not perform illegal operate of TOE and keep confidentiality of IC design information, ROM program, firmware and cryptographic keys.

  It is also assumed that firmware developer designs firmware to meet requirements from guidance documentation.
- It is assumed that the Controller is capable to establish a secure communication channel.
  The controller should have the capability of establishing a secure communication channel with TOE. This can be accomplished by mutual authentication and encryption technique. Once such a secure channel is established, the controller is authenticated and the communication is protected in confidentiality and in integrity.

4.2 Clarification of scope

The operation in Normal Mode (operation with firmware loaded in the TOE) is out of scope of the evaluation, but some of the security features provided by the TOE Security functions are also present in Normal Mode, these are: Detection of illegal operation, physical protection, and self tests.

5 Architectural Information

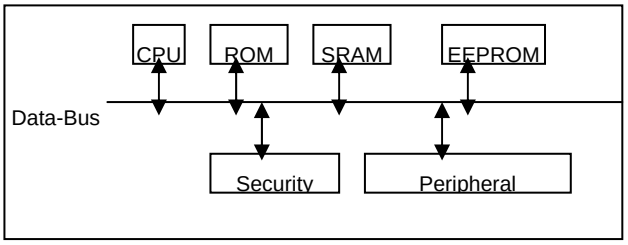

Figure 2: Block diagram of TOE

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 following documentation is provided with the product by the developer to the customer for secure usage of the TOE in accordance with the Security Target:

- RC-S940 Operation Guideline, Version 1.1, February 20, 2004 [9]
- RC-S940 IPL User's Manual, Version 1.0, March 4, 2004 [10]
- RC-S940 Administrator Tools Manual, Version 2.0, June 21, 2005 [11]

7 IT Product Testing

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

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.
- As demonstrated by [12] the developer has tested the TOE systematically at the level of TSF functionalities as given in [13].

- As demonstrated by [14] the developer has tested the TOE systematically at the level of the subsystems as given in [16] and [15].
- The entire test set comprises 756 individual test cases.

Testing result:

- All testing strategies of the TSF passed all tests of individual tests so that all TSF have been successfully tested against [17] and [15] and [16].
- 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.

During the independent testing at the developer's site the same platforms and tools as for the developer tests were used.

The results of the developer tests, which have been repeated by the evaluator, matched the results the developer.

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

The penetration testing conducted confirms that in the intended environment of use the TOE does not feature any vulnerabilities exploitable for attackers possessing a low attack potential, if taking into consideration all the measures the user is informed about.

8 Evaluated Configuration

The ST [6] only identifies one configuration of the TOE. The tests are performed with the chip RC-S940 in consistence to the configuration identified in the ST [6].

9 Results of the Evaluation

The Evaluation Technical Report (ETR), [8] 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 for those components identical with EAL4. For smart card IC specific methodology the CC supporting documents

(i) The Application of CC to Integrated Circuits

(ii) Application of Attack Potential to Smartcards

(see [4, AIS 25 and AIS 26]) and [4, AIS 20] (*Functionality classes and evaluation methodology for deterministic random number generators)* were used. The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

The verdicts for the CC, Part 3 assurance components (according to EAL4 and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		**Verdict**
Security Target evaluation	CC Class ASE	Pass
TOE description	ASE_DES.1	Pass
Security environment	ASE_ENV.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.1	Pass
PP claims	ASE_PPC.1	Pass
IT security requirements	ASE_REQ.1	Pass
Explicitly stated IT security requirements	ASE_SRE.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Configuration management	CC Class ACM	Pass
CM automation	ACM_AUT.1	Pass
CM capabilities	ACM_CAP.4	Pass
CM scope	ACM_SCP.2	Pass
Delivery and operation	CC Class ADO	Pass
Detection of modification	ADO_DEL.2	Pass
Installation, generation, and start-up procedures	ADO_IGS.1	Pass
Development	CC Class ADV	Pass
functional specification	ADV_FSP.2	Pass
high-level design	ADV_HLD.2	Pass
Implementation representation	ADV_IMP.1	Pass
low-level design	ADV_LLD.1	Pass
Representation correspondence	ADV_RCR.1	Pass
security policy model	ADV_SPM.1	Pass
Guidance documents	CC Class AGD	Pass
Administrator guidance	AGD_ADM.1	Pass
User guidance	AGD_USR.1	Pass
Life cycle support	CC Class ALC	Pass

Assurance classes and components		Verdict
development security	ALC_DVS.1	Pass
life-cycle definition	ALC_LCD.1	Pass
Tools and techniques	ALC_TAT.1	Pass
Tests	CC Class ATE	Pass
Coverage	ATE_COV.2	Pass
Depth	ATE_DPT.1	Pass
Functional tests	ATE_FUN.1	Pass
Independent testing	ATE_IND.2	Pass
Vulnerability assessment	CC Class AVA	Pass
Misuse	AVA_MSU.2	Pass
Strengh of TOE security functions	AVA_SOF.1	Pass
Vulnerability analysis	AVA_VLA.2	Pass

Table 4 Verdicts for the assurance components

The evaluation has shown that

- Security Functional Requirements specified for the TOE are Common Criteria Part 2 conformant
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL4

The following TOE Security Functions fulfil the claimed Strength of Function:

- SF1: Detection of illegal operation
- SF3: Physical protection
- SF4: Encryption of data
- SF5: Mutual authentication
- SF6: Protection of data passing through the interface

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

The results of the evaluation are only applicable to the RC-S940 with Product Code CXD9768GG and the firmware and software versions as indicated in chapter 2, table [3]

The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The guidance documents [8] - [10] contain necessary information about the usage of the TOE and all security hints therein have to be considered

No additional recommendations for the user are given.

11 Annexes

Annex A: Evaluation results regarding the development and production environment (see part D of this report).

12 Security Target

For the purpose of publishing, the security target (Public Version) [7] of the target of evaluation (TOE) is provided within a separate document. It is a public version of the complete security target [6] used for the evaluation performed.

13 Definitions

13.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CBC	Cipher Block Chaining
CC	Common Criteria for IT Security Evaluation
DES	Data Encryption Standard; symmetric block cipher algorithm
DPA	Differential Power Analysis
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
RNG	Random Number Generator

ROM	Read Only Memory
SF	Security Function
SFP	Security Function Policy

13.2 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.

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.

14 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] Applicaton Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.

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

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

[7] Security Target (Public Version) BSI-DSZ-0308-2005, Version 2.04, 13 May 2005, RC-S940 Security Target (Public Version)

[8] Evaluation Technical Report, Version 2.0, 27 June 2005 (confidential document)

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

[10] RC-S940 IPL User's Manual, Version 1.0, March 4, 2004

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

[12] Test Coverage Analysis, Version 2.0, June 1, 2005

[13] RC-S940 Interface Specification, Version 2.2, May 20, 2005

[14] Test Depth Analysis, Version 1.1, March 19, 2004

[15] High Level Design Hardware, Version 1.1, February 17, 2004

[16] High Level Design ROM Program, Version 1.3, February 12, 2004

[17] Functional Specification, Version 2.1, January 26, 2004

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 5.4) / **Final Interpretation 008**

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 Part 2 (functional requirements), 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:

Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in 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:

Assurance categorisation (chapter 2.5)

„The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class 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
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 2.1 -Assurance family breakdown and mapping“

Evaluation assurance levels (chapter 6)

„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 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 6.1)

Table 6.1 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 2 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 CC 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 6.1 - Evaluation assurance level summary“

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

„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 6.2.2)

„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 6.2.3)

„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 6.2.4)

„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 6.2.5)

„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 6.2.6)

„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 6.2.7)

„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 14.3)

AVA_SOF Strength of TOE security functions

„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 14.4)

AVA_VLA Vulnerability analysis

„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), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential.“

This page is intentionally left blank.

D Annexes

List of annexes of this certification report

This page is intentionally left blank.

Annex A of Certification Report BSI-DSZ-CC-0308-2005

Evaluation results regarding development and production environment

The IT product, RC-S940 (Target of Evaluation, TOE), produced at the Oita wafer production site[9], 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/IEC15408: 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 01. September 2005, the following results regarding the development and production environment apply. The Common Criteria assurance requirements

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

are fulfilled for the development and production sites of the TOE listed below ((a) – (g)):

(a) FeliCa Business Center, Sony Corporation (Gotenyama Site)

Role: Development of hardware / ROM Program

Gotenyama Hills 4-7-35, Kitashinagawa, Shinagawa-city, Tokyo-pref., 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) DT Fine Electronics Co., Ltd, Kawasaki factory (Kawasaki Site)

Role: Manufacture of masks

1, Komukai - Toshiba-cho, Saiwai-ku, Kawasaki-city, Kanagawa-pref., Japan

(d) DT Fine Electronics Co., Ltd, Kitakami factory (Kitakami Site)

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

Role: Manufacture of masks

6-6, Kita-kogyo-danchi, Kitakami-city, Iwate-pref., Japan

(e) Oita Factory, Toshiba Corporation (Oita Site)

Role: Manufacture of wafers

3500, Matsuoka, Oita-city Oita-pref., Japan

(f) Toshiba LSI Package Solutions Corporation (Kituki Site)

Role: Manufacture of LSI

2820-2, Minami-Kituki, Kituki-city, Oita-pref., Japan

(g) Sony EMCS Nagano Tech (Nagano Site)

Role: Initialization of the LSI / Installation of the customer's information to the LSI

5432, Toyoshina, South Azumino County, Gumma-pref., Japan

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target BSI-DSZ-0308-2005, Version 2.04, 13 May 2005, RC-S940 Security Target (confidential document) [6].

The evaluators verified, that the requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6]) are fulfilled by the procedures of these sites.