Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0379-2006

for

Renesas AE55C1 (HD65255C1) smartcard integrated circuit version 02 with ACL version 1.43 and additional SHA-256 function

from

Renesas Technology Corp.

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-0379-2006

Renesas AE55C1 (HD65255C1) smartcard integrated circuit version 02 with ACL version 1.43 and additional SHA-256 function

from

Renesas Technology Corp.

Common Criteria Arrangement
for components up to EAL4

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Part 1 Version 0.6*, *Part 2 Version 1.0* extended by advice of the Certification Body for components beyond EAL4 and 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:

PP Conformance:	**Smartcard IC Platform Protection Profile, 1.0 (BSI-PP-0002-2001)**
Functionality:	**PP-0002-2001 conformant plus product specific extensions Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL 4 augmented by:** ADV_IMP.2 (Implementation of the TSF), ALC_DVS.2 (Sufficieny of security measures), AVA_MSU.3 (Analysis and testing for insecure states) and AVA_VLA.4 (Highly resistant)

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, 15. May 2006

The President of the Federal Office
for Information Security

Dr. Helmbrecht 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)

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.

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[5]
- 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)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

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

5 Proclamation of the Bundesministerium des Innern of 22 September 2000 in the Bundesanzeiger p. 19445

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.

This evaluation contains the components ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4-components of these assurance families are relevant.

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 Renesas AE55C1 (HD65255C1) smartcard integrated circuit version 02 with ACL version 1.43 and additional SHA-256 function has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0329-2006.

The evaluation of the product Renesas AE55C1 (HD65255C1) smartcard integrated circuit version 02 with ACL version 1.43 and additional SHA-256 function was conducted by T-Systems GEI GmbH, Solution & Service Center Test Factory & Security. The T-Systems GEI GmbH, Solution & Service Center Test Factory & Security is an evaluation facility (ITSEF)[6] recognised by BSI.

The vendor and distributor is Renesas Technology Corp. The sponsor and point of contact is

Renesas Technology Europe Ltd.
Dukes Meadow Millboard Road
Bourne End
Buckinghamshire
SL8 5FH
UK

The certification is concluded with

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

This work was completed by the BSI on May 15th, 2006.

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.

---

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-22 and D-1 to D-4.

The product Renesas AE55C1 (HD65255C1) smartcard integrated circuit version 02 with ACL version 1.43 and additional SHA-256 function 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[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] Renesas Technology Corp.

Secure MCU Design Dept. 1
MCU Business Unit
Standard Product Business Group
20-1 Jousuihon-cho 5-chome
Kodaira-shi
Tokyo 187-8588, 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 Target of Evaluation (TOE) is the Renesas AE55C1 (HD65255C1) smartcard integrated circuit (IC) version 02 with ACL version 1.43 and additional SHA-256 function, produced in Naka (Japan). The TOE consists of hardware, along with IC Dedicated Test Software, some embedded software and reference and guidance documents.

The TOE was re-evaluated, because a SHA-256 function has been added.

The TOE is a hardware integrated circuit which can be used on a plastic smartcard as hardware computing platform with the Advanced Cryptographic Library (ACL) which provides cryptographic functions to the developer of Smartcard Embedded Software.

The TOE is composed of a central processing unit, a system control logic, security logic, volatile and non-volatile memories (240KBytes User ROM + 16KBytes Test ROM, 6 Kbytes RAM + 2 Kbytes Coprocessor RAM, EEPROM 32Kbytes + 8Kbytes), a 16Bit random number generator (RNG), a DES coprocessor, a Modular Multiplication Coprocessor (MMC), two interval timers, a Direct Memory Access Controller (DMAC), a watchdog timer (optional), a Firewall Management Unit (FMU), two I/O lines and an Universal Asynchronous Receiver Transmitter (UART).

The IC also provides protection features to resist leakage attacks, these include bus encryption (which is always active), memory data encryption and the ability of Smartcard Embedded Software to select noise generation and timing disturbance.

Physical security of the IC is enhanced by the presence of passive and active shielding over critical areas and by the use of design techniques that obscure the function and operation of the physical layout.

The TOE includes the IC Dedicated Test Software which is integrated into a TOE hardware. It is used for mode transition and testing during IC production and is not available for users.

The ACL, the ROM and the IC Dedicated Test Software, which is implemented on hardware, are part of the TOE. Apart from this the Smartcard Embedded Software (e.g. an operating system) is not part of the TOE.

The Security Target [6] is written using the Smartcard IC Platform Protection Profile [7]. With reference to this Protection Profile, the smartcard product lifecycle is described in 7 phases. The development, production and operational user environment are described in reference to these phases. TOE delivery is defined at the end of phase 3 or phase 4.

The assumptions, threats and objectives defined in this Protection Profile [7] are used. To address additional security features of the TOE (e.g. cryptographic services), the security environment as outlined in the PP [7] is augmented by an additional policy, threats, assumptions and security objectives accordingly.

The IT product Renesas AE55C1 (HD65255C1) smartcard integrated circuit version 02 with ACL version 1.43 and additional SHA-256 function was evaluated by T-Systems GEI GmbH, Solution & Service Center Test Factory & Security. The evaluation was completed on April 26th,2006. The T-Systems GEI GmbH, Solution & Service Center Test Factory & Security is an evaluation facility (ITSEF)[8] recognised by BSI.

The vendor and distributor is Renesas Technology Corp. The sponsor and point of contact is

Renesas Technology Europe Ltd.
Dukes Meadow Millboard Road
Bourne End
Buckinghamshire
SL8 5FH
UK

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 EAL 4+ (Evaluation Assurance Level 4 augmented). The following table shows the augmented assurance components.

Requirement	**Identifier**
EAL4	TOE evaluation: methodically designed, tested, and reviewed
+ ADV_IMP.2	Development – Implementation of the TSF
+ ALC_DVS.2	Life cycle support – Sufficiency of security measures
+ AVA_MSU.3	Vulnerability assessment - Analysis and testing for insecure states
+ AVA_VLA.4	Vulnerability assessment - Highly resistant

Table 1: Assurance components and EAL-augmentation

1.2 Functionality

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

The following SFRs are taken from CC part 2. The source of this SFRs is the Protection Profile BSI-PP-0002-2001 [PP, 7], the “Smartcard Integrated Circuit Platform Augmentations” [PA, 8] or they are added in the Security Target [ST, 6]:

[8] Information Technology Security Evaluation Facility

Security Functional Requirement	Addressed issue	Source from PP, PA or added in ST
FCS	**Cryptographic support**	
FCS_COP.1 [3DES]	Cryptographic operation	PA
FCS_COP.1 [RSA]	Cryptographic operation	PA
FCS_COP.1 [SHA-1]	Cryptographic operation	PA
FCS_COP.1 [SHA-256]	Cryptographic operation	PA
FCS_COP.1 [RIPEMD-160]	Cryptographic operation	PA
FCS_CKM.1 [RSA]	Cryptographic key generation	PA
FDP	**User data protection**	
FDP_ITT.1 [HW]	Basic internal transfer protection	PP
FDP_ITT.1 [ACL]	Basic internal transfer protection	PP
FDP_IFC.1 [HW]	Subset information flow control	PP
FDP_IFC.1 [ACL]	Subset information flow control	PP
FDP_ACC.1 [CRP]	Subset access control	ST
FDP_ACC.1 [WPP]	Subset access control	ST
FDP_ACF.1 [CRP]	Security attribute based access control	ST
FDP_ACF.1 [WPP]	Security attribute based access control	ST
FPT	**Protection of the TOE Security Functions**	
FPT_FLS.1	Failure with preservation of secure state	PP
FPT_SEP.1	TSF domain seperation	PP
FPT_PHP.3	Resistance to physical attack	PP
FPT_ITT.1 [HW]	Basic internal TSF data transfer protection	PP
FPT_ITT.1 [ACL]	Basic internal TSF data transfer protection	PP
FRU	**Resource utilisation**	
FRU_FLT.2	Limited fault tolerance	PP

Table 2: SFRs for the TOE taken from CC Part 2

The following CC part 2 extended SFRs are defined:

Security Functional Requirement	**Addressed issue**	**Source from PP, PA or added in ST**
FAU	**Security audit**	
FAU_SAS.1	Audit storage	PP
FCS	**Cryptographic support**	
FCS_RND.1 [TRNG]	Quality metric for random numbers	PP
FCS_RND.1 [PRNG]	Quality metric for random numbers	PP
FMT		
FMT_LIM.1		PP
FMT_LIM.2		PP

Table 3: SFRs for the TOE, CC part 2 extended

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST [6] chapter 5.1.

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

TOE Security Function	**Addressed issue**
SF.HWProtect	HW protection The TOE is protected from attacks on the operation of the IC hardware. The protection includes high and low voltage, clock frequency and temperature detection and detection of illegal access and instruction. It also includes RNG failure detection, shielding and memory layout scrambling, memory address encryption and memory data encryption for ROM.
SF.LeakProtect	Leakage protection The TOE hardware protects against leakage of information from the IC. The protection features include data and address bus encryption, noise generation, time disturbance and DES protection.
SF.ACL-LeakProtect	ACL leakage protection The ACL provides additional measures to protect against leakage of information from the IC. The protection features include scrambled copy/ compare/ XOR and secure RSA operation and keyset generation, secure modular inversion and secure multiply.
SF.RNG	Random Number Generator The RNG is designed to produce random numbers for the generation of cryptographic keys and for other critical uses.

TOE Security Function	Addressed issue
	This RNG meets the requirements of application class P2 as specified in [4, AIS31]. Moreover the ACL includes a function to access the HW RNG, which automatically runs an online test of the HW RNG to verify that its operation has not been compromised. This function implements „Poker Test“ according to [4]. The TOE also includes the software implementations of a pseudo random number generator (PRNG). This PRNG is implemented according to the standard ANSI X9.31 Appendix A and meets functionality class K3 as specified in the AIS20.
SF.DES	DES coprocessor The TOE provides a hardware DES coprocessor that carries out DES encryption and decryption in ECB mode and ACL software functions to access this coprocessor for DES and implement Triple-DES, according to the FIPS PUB 46-3 standard [16]. Moreover the ACL provides an interface function for the DES coprocessor and in addition implements a triple DES function. The DES and 3DES algorithm are implemented according to FIPS PUB 46-3. Only 3DES has sufficient SOF to be claimed as a SF and for use in the secure part of any Smartcard Embedded Software.
SF.FMU	Firewall Management Unit The FMU enables software to control addresses that can be accessed to check that a target address used in any instruction is within specified limits and if not to enter the reset state or FMU interrupt. In addition the FMU may enforce a policy controlled only by software executing in ROM, that the TOE may not execute code either EEPROM or RAM or both.
SF.ESFunctions	The Smartcard Embedded Software developer can rely on the following TOE functionality that has been specifically evaluated as part of the TOE • Generation of non-maskable interrupt (the EWE interrupt) when writing the EEPROM • CPU halt initiated by user software to stop executation until an external reset is received
SF.TestModeControl	Test Mode Control If the TOE has been set to user mode, test mode functions are no longer accessible.
SF.EEPAccess	EEPROM Access The TOE allows any page of EEPROM to have writes (or erase) disallowed by setting the page to have a protect state. If a write (or erase) is attempted to a protected page then it will leave the page content unaltered. This protection is permanent once set.
SF.Inject	Injection

TOE Security Function	Addressed issue
	Each TOE is injected with data that uniquely identifies the individual IC during manufacture. If specified for the Smartcard Embedded Software included, then additional data may also be injected during manufacture.
SF.MMCopro	The TOE provides coprocessor that carries out modular multiplication. This forms the basis for software implementation of algorithms such as RSA. The ACL provides an implementation of the RSA and RSA CRT algorithm using the hardware MMC. It also provides secure generation of keys for the RSA and RSA CRT algorithm using the hardware RNG and software PRNG. The RSA and RSA CRT encryption, decryption and key generation of the ACL clear all parts of the MMC of intermediate results, keys and key parts immediately before returning control of the calling environment.
SF.Hash	Hash functions The ACL provides implementations of the hash functions SHA-1, SHA-256 and RipeMD-160 according to the FIPS PUB 180-2 and ISO/IEC 10118-3:2003 respectively.

Table 4: TOE Security Functions

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

1.3 Strength of Function

The TOE's strength of functions is claimed "high" (SOF-high) for specific functions as indicated in the Security Target [6, chapter 5.1.4].

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.

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

The threats which were assumed for the evaluation and averted by the TOE and the organisational security policies defined for the TOE are specified in the Security Target [6] and can be summarized as follows.

It is assumed that the attacker is a human being or process acting on behalf of the human being.

With reference to the Protection Profile [7], the Security Target [6] defines so-called standard high level security concerns derived from considering the end-usage phase (phase 7 of the lifecycle as described in the Security Target) as follows:

- Manipulation of User Data and of the Smartcard Embedded Software (while being executed/processed and while being stored in the TOE´s memories),
- Disclosure of User Data and of the Smartcard Embedded Software (while being processed and while being stored in the TOE´s memories) and
- Deficiency of random numbers.

These high-level security concerns are refined by defining threats on a more technical level for

- Inherent information leakage
- Physical probing
- Physical manipulation
- Malfunction due the Environmental Stress
- Forced Information leakage
- Abuse of Functionality
- Deficiency of Random Numbers

Phase 1 and the phases from the TOE delivery up to the end of phase 6 are covered by assumptions (see below).

The development and production environment starting with phase 2 up to the TOE delivery is covered by an organisational security policy outlining that the IC Developer/Manufacturer must apply the policy “Protection during TOE development and production (P.Process-TOE)” so that no information is unintentionally made available for the operational phase of the TOE. The Policy ensures confidentiality and integrity of the TOE and its related design information and data. Access to samples, tools and material must be restricted.

Additionally, the Security Target defines the security concern about specific attacks on the Smartcard Embedded Software the TOE is not able to detect or to respond to. This concern is detailed in terms of the threats.

- Inability of the TOE to detect an attack and
- Inability of the Smartcard Embedded Software to respond to an attack

A specific additional security functionality for DES encryption and decryption must be provided by the TOE according to an additional security policy defined in the Security Target.

Objectives are taken from the Protection Profile plus additional ones related to the additional threats and policy.

1.5 Special configuration requirements

The TOE has two different operating modes, user mode and test mode. The application software being executed on the TOE cannot use the test mode. The TOE is delivered as a hardware unit at the end of the IC manufacturing process

(Phase 3) or at the end of the IC packaging (Phase 4). At this point in time the operating system software is already stored in the non-volatile memories of the chip and the test mode is disabled. Thus there are no special procedures for generation or installation that are important for the secure use of the TOE. The further production and delivery processes, like the Smartcard finishing process, personalization and the delivery of the Smartcard to an enduser, have to be organized in a way that excludes all posibilities of physical manipulation of the TOE. 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 and the requirements on the software have to be applied as described in the user documentation.

1.6 Assumptions about the operating environment

Since the Security Target claims conformance to the Protection Profile [7], the assumptions defined in section 3.2 of the Protection Profile are valid for the Security Target of this TOE. With respect to the life cycle defined in the Security Target, phase 1 and the phases from TOE delivery up to the end of phase 6 are covered by these assumptions from the PP.

The developer of the Smartcard Embedded Software (phase 1) must ensure:

- The apropriate „usage of hardware platform (A.Plat-Appl)“ while developing this software in phase 1. Therefore it has to be ensured that the software fulfils the assumptions for a secure use of the TOE. In particular the assumptions imply the developers are trusted to develop software that fulfils the assumptions.
- The apropriate „treatment of the user data (A.Resp-Appl)“ while developing this software in phase 1. The smartcard operating system and the smartcard application software have to use security relevant user data (especially keys and plain text data) in a secure way. It is assumed that the Security Policy as defined for the specific application context of the environment does not contradict the Security Objectives of the TOE. Only appropriate secret keys as input for the cryptographic function of the TOE have to be used to ensure the strength of cryptographic operation.

Protection during packaging, finishing and personalization (A.Process-Card) is assumed after TOE delivery up to the end of phase 6, as well as during the delivery to phase 7.

Following additional assumptions are defined in the Security Target:

- Key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks (A.Key-Function).
- Date for injection/pre-personalization will be supplied from the various bodies controlling the operations of the system in which the TOE will be used. It is assumed that the generation, distribution, maintenance and destruction of these data is adequately secure (A.InjDatSupp).

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

The Target of Evaluation (TOE) is called Renesas AE55C1 (HD65255C1) smartcard integrated circuit version 02 with ACL version 1.43 and additional SHA-256 function .

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	AE55C1 (HD65255C1) Smartcard Integrated Circuit	02	Wafer or package module
2	SW	IC Dedicated Test Software Test ROM software	1.4	Included in AE55C1 Test ROM
3	SW	ACL (Advanced Cryptographic Library)	1.43	Software module (this is implemented in the Embedded Software by the User)
4	SW	SHA-256 software	1.10	Software module (this is implemented in the Embedded Software by the User)
5	DOC	Hardware Manual	1.0	Hardcopy
6	DOC	User Guidance	4.40	Hardcopy
7	DOC	Cryptographic Library Manual	1.70	Hardcopy
8	DOC	Cryptographic Library Manual (SHA-256)	1.01	Hardcopy
9	DOC	Option List	1.3	Electronic data/ Hardcopy

Table 5: Deliverables of the TOE

The TOE is identified by HD65255C1 smartcard integrated circuit (short form AE55C1), Version 02 (stored as a version number in the EEPROM) with ACL version 1.43 and additiona SHA-256 function produced in Naka (indicated by IC manufacturers ID number 4870 for Naka). The pre-personalization using the option list [11].

To ensure that the customer receives this evaluated version, the delivery procedures described in [10] have to be followed.

3 Security Policy

The security policy of the TOE is to provide basic security function to be used by the smartcard operating system and the smartcard application thus providing an overall smartcard system security. Therefore, the TOE will implement a symmetric cryptographic block cipher algorithm to ensure the confidentiality of plain text data by encryption and to support secure authentification, protocols and it will provide a random number generation of appropriate quality.

As the TOE is a hardware security platform, the security policy of the TOE is also to provide proctection against leakage of information (e.g. to ensure the confidentiality of cryptographic keys during cryptographic functions performed by the TOE), against physical probing, against malfunctions, against physical manipulations and against abuse of functionality. Hence the TOE shall:

- Maintain the integrity and the confidentiality of data stored in the memory of the TOE and
- Maintain the integrity, the correct operation and the confidentiality of security functions (security mechanism and associated functions) provided by the TOE.

4 Assumptions and Clarification of Scope

The smartcard operating system and the application software stored in the user ROM and in the EEPROM are not part of the TOE. The code in the Test ROM of the TOE (IC Dedicated Software) is used by the TOE manufacturer to check the chip function before TOE delivery. This was considered as part of the evaluation under the CC assurance aspects ALC for relevant procedures and under ATE for testing.

The TOE is delivered as a hardware unit at the end of the chip manufacturing process (phase 3 of the life cycle defined) or at the end of the IC packaging into modules (phase 4 of the life cycle defined). At these specific points in time the operating systems software is already stored in the non-volatile memories of the chip and the test mode is completely disabled.

The smartcard applications need the security functions of the smartcard operating system based on the security features of the TOE. With respect to security the composition of this TOE, the operating system and the smartcard application is important. Within this composition the security functionality is only partly provided by the TOE and causes dependencies between the TOE security functions and the functions provided by the operating system or the smartcard application on top. These dependencies are expressed by environmental and secure usage assumptions as outlined in the user documentation.

Within this evaluation of the TOE several aspects were specifically considered to support a composite evaluation of the TOE together with an embedded smartcard application software (i.e. smartcard operating system and application). This was necessary as Renesas Technology Corp. is the TOE

developer and manufacturer and responsible for specific aspects of handling the embedded smartcard application software in its development and production environment. For those aspects refer to chapter 9 of this report.

5 Architectural Information

The Renesas AE55C1 (HD65255C1) smartcard integrated circuit version 02 with ACL version 1.43 and additional SHA-256 function providing a hardware platform to a smartcard operating system and smartcard application software. The top level block diagram and the list of subsystems can be found within the TOE description of the Security Target. The complete hardware description and the complete instruction set of the Renesas AE55C1 (HD65255C1) smartcard integrated circuit version 02 with ACL version 1.43 and additional SHA-256 function is to be found in the Hardware Manual [12], the ACL User Manual (ACLSM) [13] and in the ACL User Manual (SHA-256) [14].

For the implementation of the TOE security functions basically the components CPU, EEPROM, ROM, RAM, system control registers, DES coprocessor, Firewall Management Unit, a random number generator, the analog block with security sensors, the random logic module for security logic and the ACL are used. Security measures for physical protection are realised within the layout of the whole circuitry.

The TOE IC Dedicated Software, stored on the chip, is used for testing purposes during production only and is completely separated from the use of the embedded software by disabling before TOE delivery.

6 Documentation

The following documentation is provided with the product by the developer to the customer (see also table 5 of this report)

- Hardware Manual, Version 1.00, Hardcopy
- User Guidance, Verison 4.40, Hardcopy
- Cryptographic Library Manual, Version 1.70, Hardcopy
- Cryptographic Library Manual (SHA-256), Version 1.01, Hardcopy
- Option List, Version 1.3, Electronic data/ Hardcopy

7 IT Product Testing

The tests performed by the developer were divided into five categories:

- tests which are performed in a simulation environment;
- functional production tests, which are done as a last step of the production process (phase 3) and in case TOE delivery is at the end of phase 4, additionally done as a last step of IC Packaging. These tests are done for every chip to check its correct functionality;

- characterization tests, which were used to determine the behaviour of the chip with respect to different operating conditions;
- special verification tests for security functions which were done with samples of the TOE and
- layout checks, tests that are executed to verify the correspondence between the logic circuit data and the chip design data.

The developer tests cover all security functions and all security mechanisms as identified in the functional specification and the high level design. Chips from the production site in Naka (see Annex A of this report) were used for tests.

The evaluators could repeat the tests of the developer either using the library of programs and tools delivered to the evaluator or at the developer site, except (v). The performed independent tests to supplement, augment and to verify the tests performed by the developer by sampling. Besides repeating exactly the developer tests, test parameters were varied and additional analysis was done. Security features of the TOE realised by the specific design and layout measures were checked by the evaluators during layout inspections.

The evaluators gave evidence that the actual version of the TOE (Version 02 with IC manufacturer´s ID number 4870 for Naka) provides the security functions as specified. The test results confirm the correct implementation of the TOE security functions.

For penetration testing the evaluators took all security functions into consideration. Intensive penetration testing was performed to consider the physical tampering of the TOE using highly sophisticated equipment and expert know-how.

8 Evaluated Configuration

The TOE identified by Renesas AE55C1 (HD65255C1) smartcard integrated circuit version 02 with ACL version 1.43 and additional SHA-256 function, manufacturer´s ID number 4870 for Naka. There is only one evaluated configuration of the TOE. This configuration (all TSF are active and usable) has to be selected by the customer in the option list at order. All information of how to use the TOE and ist security functions by the software is provided within the user documentation.

The TOE has two different operating modes, user mode and test mode. The application software being executed on the TOE can not use the test mode. Thus, the evaluation was mainly performed in the user mode. However, some evalution activities were performed in the test mode. For those cases, a rational was provided why the results are also valid for the user mode.

9 Results of the Evaluation

9.1 Evaluation of the TOE

The Evaluation Technical Report (ETR) [9] 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 components beyond EAL4 the methodology was defined in co-ordination with the Certification Body.

For smart card IC specific methodology the CC supporting documents

- *Joint Interpretation Library - The application of CC to integrated circuits*
- *Joint Interpretation Library - Integrated Circuit Hardware Evaluation Methodology, Vulnerability Assessment*
- *Functionality classes and evaluation methodology for physical random number generators*
- *Functionality classes and evaluation methodology for deterministic random number generators*

(see [4] AIS 20, AIS 25, AIS 26 and AIS 31) 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 EAL 4 augmented 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
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS

Assurance classes and components		**Verdict**
Problem tracking CM coverage	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
Fully defined external interface	ADV_FSP.2	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Implementation of the TSF	ADV_IMP.2	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Information correspondence demonstration	ADV_RCR.1	PASS
Informal TOE 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
Sufficiency of security measures	ALC_DVS.2	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Well defined development tools	ALC_TAT.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Analysis and testing for insecure states	AVA_MSU.3	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Highly resistant	AVA_VLA.4	PASS

Table 6: Verdicts for the assurance components

The evaluation has shown that:

- the TOE is conform to the Protection Profile BSI-PP-0002-2001
- Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL4 augmented by ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4

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

  SF.LeakProtect,
  SF.ACL-LeakProtect,
  SF.RNG and
  SF.Hash.

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 SF.DES and for other usage of encryption and decryption within the TOE.

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

The code in the Test ROM of the TOE (IC dedicated software) is used by the TOE manufacturer to check the chip function before TOE delivery. This was considered as part of the evaluation under the CC assurance aspects ALC for relevant procedures and under ATE for testing.

The results of the evaluation are only applicable to the Renesas AE55C1 (HD65255C1) smartcard integrated circuit version 02 with ACL version 1.43 and additional SHA-256 function produced in Naka (indicated by IC manufacturer´s ID number 4870 for Naka).

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.

9.2 Additional evaluation results

To support the composite evaluation of the TOE together with a specific smartcard embedded software, additional evaluator actions were performed during the TOE evaluation. The results are documented in the ETR-lite [18]. Therefore, refering to the life-cycle model for the TOE the interaction between phase 1 and phase 2 is of importance and the interface between the smartcard embedded software developer and the developer of the TOE was examined.

10 Comments/Recommendations

1. The operational documentation [10], [12], [13], [14] contains necessary information about the usage of the TOE. For secure usage of the TOE the fulfilment of the assumptions about the environment in the Security Target has to be taken into account. These requirements are stated in the guidance document [10].
2. For evaluation of products or systems including the TOE as part or using the TOE as a platform (e.g. smartcard operating systems or complete

smartcards), specific information resulting from this evalution is of importance and shall be given to the succeeding evaluation.

3. The TOE software for random number postprocessing shall be implemented by the embedded software developer as outlined in the guidance [10].

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 [6] of the target of evaluation (TOE) is provided within a separate document. It is a sanitized version of the complete Security Target [17] used for the evaluation performed.

13 Definitions

13.1 Acronyms

3DES	see Triple-DES
ACL	Advanced Cryptographic Library
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CC	Common Criteria for IT Security Evaluation
CPU	Central Processing Unit
DES	Data Encryption Standard
DMAC	Direct Memory Access Controller
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
FMU	Firewall Management Unit
HW	Hardware
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MMC	Modular Multiplication Coprocessor
PP	Protection Profile
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory

RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest, Shamir, Adelmann - a public key encryption algorithm
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
SW	Software
TOE	Target of Evaluation
Triple-DES	Symmetric block cipher algorithm based on DES
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UART	Universal Asynchronous Receiver Transmitter

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.

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.

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

AIS 20, Version 1, 02 Dezember 1999 for: Functionality classes and evaluation methodology of deterministic random number generators

AIS 25, Version 2, 29 July 2002 for: CC Supporting Document, The Application of CC to Integrated Circuits, Version 1.2, July 2002

AIS 26, Version 2, 6 August 2002 for: CC Supporting Document, Application of Attack Potential to Smartcards, Version 1.1, July 2002

AIS 31, Version 1, 25 September 2001 for: Functionality classes and evaluation methodology of physical random number generators

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

[6] Security Target BSI-DSZ-0379-2006, Version 15.0, 29 March 2006, AE55C1 (HD65255C1) Version 02 with ACL version 1.43 Smartcard Security Target, Renesas Technology Corp. (confidential document)

[7] Protection Profile BSI-PP-0002-2001, Version v1.0, Smartcard IC platform Protection Profile, July 2001, Eurosmart

[8] Smartcard Integrated Circuit Platform Augmentations, v1.0, Atmel, Hitachi Europe, Infineon Technologies & Philips Semiconductors, March 2002

[9] Evaluation Technical Report, Version 1.0, April 25, 2006, Evaluation Technical Report BSI-DSC-CC-0379 (confidential document)

[10] Renesas 32-bit Smart Card Microcomputer AE-5 Series User Guidance Manual, Rev. 4.40, Renesas Technology, 27 January 2006 (confidential document)

[11] Option List for Smart Card Microcomputer (for HD65255C1 [AE55C1]), v.1.3, Renesas Technology Corp., 06 February 2006

[12] AE55C1 Hardware Manual, Renesas Technology, Rev. 1.00, 15 March 2005

[13] AE-5 Series Cryptographic Library, Renesas Technology, User´s Manual, Rev. 1.70, 27 January 2006

[14] AE-5 Series Cryptographic Library (SHA-256), Renesas Technology, User´s Manual, User's Manual Appendix Rev. 1.01, 15 March 2006

[15] FIPS PUB 180-2 Federal Information Processing Standards Publication Secure Hash Standard, 01 August 2002

[16] FIPS PUB 46-3 Federal Information Processing Standards Publication Data Encryption Standard (DES), Reaffirmed 25 Oct. 1999

[17] Security Target BSI-DSZ-0379-2006, Version 5.0, 7 April 2006, AE55C1 (HD65255C1) Version 02 with ACL version 1.43 Smartcard Security Target, Public Version, Renesas Technology Corp.

[18] Evaluation Technical Report lite, Version 1.0, 10 May 2006, ETR-lite for composition according to AIS36 (confidential document)

[19] Certification Report BSI-DSZ-CC-0329-2006 for Renesas AE55C1 (HD65255C1) smartcard integrated circuit version 02 with ACL version 1.43, March 28th, 2006

This page is intentionally left blank.

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 1: Assurance family breakdown and map

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 2: 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.“

D Annexes

List of annexes of this certification report

This page is intentionally left blank.

Annex A of Certification Report BSI-DSZ-CC-0329-2006

Evaluation results regarding development and production environment

The IT product Renesas AE55C1 (HD65255C1) smartcard integrated circuit version 02 with ACL version 1.43 and additional SHA-256 function (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 components beyond EAL4 and 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 May 15th, 2006, the following results regarding the development and production environment apply. The Common Criteria 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.2, ALC_LCD.1, ALC_TAT.1),

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

a) Renesas Technology Corp. - Musashi site, 5-20-1 Jousuihon-cho, Kodaira-shi, Tokyo, Japan (short name: Musashi)

b) Renesas Technology Corp. - Naka Site, 751 Horiguchi, Hitachinaka-shi, Ibaraki Pref., Japan (short name: Naka), (wafer fab)

c) Dai Nippon Printing Co., Ltd., 2-2-1 Fukuoka, Fujimino-shi, Saitama Pref., Japan (short name: DNP)

d) Hitachi ULSI Systems Co., Ltd. - Plaza site, 5-22-1 Jousuihon-cho, Kodaira-shi, Tokyo, Japan

e) Renesas Technology Corp. - Kofu site, 4617 Kai-shi, Yamanashi Pref., Japan (short name: Kofu)

f) Renesas High Qualities, Inc., 4617 Kai-shi, Yamanashi Pref., Japan (short name: RHQ)

g) Toyo Electronics Co., Ltd., 2781-1 Shimosone-cho, Kofu-shi, Yamanashi 400-1508, Japan (short name: Toyo)

h) MTEX Matsumura Corp., 2-2-2 Kitamachi, Obanazawa-shi, Yamagata Pref., Japan (short name: MTEX)

i) Renesas Technology Europe GmbH - Munich site, Dornbacher Straße 3, 85622 Feldkirchen bei München, Germany (short name: Munich)

j) Renesas Technology Europe Ltd., Dukes Meadow, Millboard Road, Bourne End, Buckinghamshire, SL8 5FH, U.K.

The hardware part of the TOE produced at site (b) (Naka) is indicated by IC manufacturer´s ID number 4870.

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target (Security Target BSI-DSZ-0379-2006, Version 15.0, 29 March 2006, AE55C1 (HD65255C1) Version 02 with ACL version 1.43 and additional SHA-256 function Smartcard Security Target, Renesas Technology Corp. (confidential document)).

The evaluators verified, that the threats and the security objectives for the life cycle phases 2, 3 and 4 up to delivery at the end of phases 3 or 4 as stated in the Security Target [6] are fulfilled by the procedures of these sites.