Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0873-2014

for

Renesas RCL3.0 (version 5897) on RS4FC128 Version 01 integrated circuit Product Type Code 00 and Renesas RCL3.0 (version 5897) on RS4FC128E Version 01 integrated circuit Product Type Code 01

from

Renesas Electronics Corporation

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0873-2014

Smartcard Controller

Renesas RCL3.0 (version 5897) on RS4FC128 Version 01 integrated circuit Product Type Code 00 and Renesas RCL3.0 (version 5897) on RS4FC128E Version 01 integrated circuit Product Type Code 01

from	Renesas Electronics Corporation
PP Conformance:	Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5

Common Criteria
Recognition
Arrangement
for components up to
EAL 4

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 5 March 2014

For the Federal Office for Information Security

Bernd Kowalski
Head of Department

L.S.

SOGIS Recognition
Agreement

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

Contents

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

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 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

[2] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

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

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

[5] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

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

2.2 International Recognition of CC – Certificates (CCRA)

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

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

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

This evaluation contains the components ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, ATE_DPT.3 and AVA_VAN.5 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 RCL3.0 (version 5897) on RS4FC128 Version 01 integrated circuit Product Type Code 00 and Renesas RCL3.0 (version 5897) on RS4FC128E Version 01 integrated circuit Product Type Code 01 has undergone the certification procedure at BSI.

The evaluation of the product Renesas RCL3.0 (version 5897) on RS4FC128 Version 01 integrated circuit Product Type Code 00 and Renesas RCL3.0 (version 5897) on RS4FC128E Version 01 integrated circuit Product Type Code 01 was conducted by T-Systems GEI GmbH. The evaluation was completed on 6 February 2014. T-Systems GEI GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Renesas Electronics Corporation.

The product was developed by: Renesas Electronics Corporation.

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

[6] Information Technology Security Evaluation Facility

4 Validity of the Certification Result

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

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

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

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

5 Publication

The product Renesas RCL3.0 (version 5897) on RS4FC128 Version 01 integrated circuit Product Type Code 00 and Renesas RCL3.0 (version 5897) on RS4FC128E Version 01 integrated circuit Product Type Code 01 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Renesas Electronics Corporation
5-20-1 Jousuihon-cho, Kodaira-shi
Tokyo 187-8588
Japan

This page is intentionally left blank.

B Certification Results

The following results represent a summary of

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

1 Executive Summary

The Target of Evaluation (TOE) is Renesas RCL3.0 (version 5897) on RS4FC128 Version 01 integrated circuit Product Type Code 00 and Renesas RCL3.0 (version 5897) on RS4FC128E Version 01 integrated circuit Product Type Code 01.

The composite TOE is a cryptographic library running on the Renesas' certified hardware platform RS4FC128(E) security integrated circuit Version 01. As software library, the RCL3.0 has to be integrated in an application software (Security IC Embedded Software) running on the hardware platform.

The TOE complies with the Security IC Platform Protection Profile, where the cryptographic library serves as IC Dedicated Support Software as defined in [7]. It provides cryptographic services using the certified hardware platform RS4FC128(E).

The TOE consists of the certified hardware platform and the cryptographic library software. The hardware platform is intended for use in a variety of security applications requiring large memory, high security and high speed secure authentication, data encryption, or electronic signature generation. The hardware platform is described in the related certification report.

The cryptographic library software is intended for use by the Security IC Embedded Software. It comprises the following major blocks: Public Key Algorithm Library (PKLIB), Secret Key Algorithm Library (SKLIB), and Common Code Platform Library (CCPLIB).

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007 [7].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [8], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
SF.RCL-LeakProtect	Leak Protection
SF.RNG	Random Number Generator
SF.DES	Triple-DES function
SF.AES	AES function
SF.PKCC	RSA functions

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [8], chapter 7.1.

The assets to be protected by the TOE are defined in the Security Target [6] and [8], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of

Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [8], chapter 3.2, 3.3 and 3.4.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

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 RCL3.0 (version 5897) on RS4FC128 Version 01 integrated circuit Product Type Code 00 and Renesas RCL3.0 (version 5897) on RS4FC128E Version 01 integrated circuit Product Type Code 01

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Renesas RS4FC128(E) integrated circuit Version 01	Version 01	wafer, Chip On Tape (COT), SON8
2	SW	IC Dedicated Test Software, Test ROM software	Version 50282	included in the TOEs ROM
3	SW	Secure Boot Loader software	Version 5560	included in the TOEs ROM
4	DOC	RNG on-line test software printed on the guidance document (cf. [17])	Version 1.1	source code printed in the guidance document
5	SW	Renesas Cryptographic Library 3.0	Version 5897	as electronic copy
6	DOC	RS4FC128, RS4FC128E User's Manual: Hardware, Renesas Secure Microcomputer RS-4E Series, July 2013 [16]	Revision 1.00	as hardcopy or electronic copy
7	DOC	Secure Boot Loader Version 5560 User's Manual: Hardware, Renesas Secure Microcomputer RS-4E Series, August 2013 [18]	Revision 1.10 Document Number R01US0044EJ0110	as hardcopy or electronic copy
8	DOC	RS-4E Series User Guidance Manual, September 2013 [17]	Revision 1.1	as hardcopy or electronic copy
9	DOC	Option List for Smart Card Microcomputer (for RS4FC128), 16 November 2012 [14]	Version 0.2 Revision 22272	as hardcopy or electronic copy
10	DOC	Renesas Cryptographic Library 3, User's Manual: Software, Renesas Secure Microcomputer RS-4E Series, 25 September 2013 [15]	Version 5897 Revision 1.10 Document Number R01US0043EJ0110	as hardcopy or electronic copy

Table 2: Deliverables of the TOE

Only 7 items (the hardware platform, five documents, and the electronic RCL3.0 software) are delivered since the IC Dedicated Software and the Secure Boot Loader software included in the ROM is delivered on the chip and the RNG on-line test software is printed in the guidance document [17].

The TOE hardware platform RS4FC128 is available as wafers or as packaged module. The security functionality of the TOE is not influenced by the delivery forms.

Product Name	Product Type Code	Application	Package at shipment
RS4FC128	00	Smart cards	Wafer, COT
RS4FC128E	01	Embedded in devices	Wafer, SON8

Table 3: Configurations of the TOE

The commercial type name of the underlying hardware is the name of the RS4FC128(E) along with the selected product type code, which is described in [14]. The package at shipment is selected by the customers in [14]. The commercial type name of the RCL library is Renesas Cryptographic Library 3.0 (RCL3.0) Version 5897.

The underlying hardware platform is identified as described in [14]. The user is required to verify the integrity of the RCL using SHA-256 hash calculation. The RCL is delivered as three libraries and one header file (refer to section 1.2 of [15]). The identification occurs by comparison of their calculated SHA-256 values with the hash values depicted in section 2.3.8 of [15].

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues: The security policy of the TOE is to provide basic Security Functions to be used by the smart card operating system and the smart card application thus providing an overall smart card system security. Therefore, the TOE will implement algorithms to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols and it will provide a random number generator.

The security policy of the TOE is also to provide protection 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 Features provided by the TOE.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

Name	Assumption Title
OE.Plat-Appl	Usage of Hardware Platform
OE.Resp-Appl	Treatment of User Data
OE.Process-Sec-IC	Protection during composite product manufacturing
OE.InjDatSupp	Injected Data Support

Table 4: Objectives for the TOE-Environment

Details can be found in the Security Target [6] and [8], chapter 4.2.

5 Architectural Information

The composite TOE comprises Renesas Cryptographic Library RCL3.0 running on Renesas' security IC RS4FC128 and packaged version RS4FC128E. The TOE complies with the Security IC Platform Protection Profile [7]. The RCL3.0 as cryptographic library provides cryptographic services using the certified hardware platform RS4FC128 with countermeasures against attacks described in RCL3.0 on RS4FC128 Version 01 Security Target [6]. These may be incorporated into the user's security IC embedded software.

The hardware platform is Renesas' Security IC RS4FC128 and packaged version RS4FC128E, which has already been certified according the requirements of CC EAL5+ (refer to [12]). It implements different security measures and requires the software to implement further countermeasures. The requirements are described in RS-4E Series User Guidance Manual [12] and Secure Boot Loader Version 5560, User's Manual: Hardware [15].

The RCL3.0 is provided as three different libraries (PKLIB, SKLIB, CCPLIB), which provide the following functions in a secured implementation to protect against inherent leakage:

Public Key Algorithm library (PKLIB):

- RSA CRT algorithm,
- RSA public algorithm,
- Multiplication of data blocks containing secret integers, based on the hardware PKCC and using data blinding,
- Comparison: To compare data blocks containing secret integers, the RCL3.0 provides a function to perform the operation, based on the hardware PKCC and using data blinding. In contrast to the equality test function from the CCPLIB, the supported data block length is different and the function checks whether the first input integer is equal to, smaller or larger than the second input integer.

Secret Key Algorithm library (SKLIB):

- DES keys loading process,
- 3DES algorithm in ECB, CBC and OFB modes using the hardware DES coprocessor,
- AES keys loading process,
- AES algorithm in ECB, CBC and OFB modes using the hardware AES coprocessor.

Common Code Platform library (CCPLIB):

- Online test of the underlying platform's hardware random number generator (without security claim),
- Random data string generation based on the underlying 16-bit hardware random number generator,
- Scrambled copy / equal / XOR: To copy, test for equality or compute the XOR sum of data blocks containing secret information, the RCL3.0 provides functions to perform the operation in a varying order. In contrast to the compare function from the PKLIB, the scrambled equality test function only tests for equality and the supported data block length is different,
- Scrambled 32-bit check sum: To compute a 32-bit check sum over a given data block containing secret information, the RCL3.0 provides a function to perform the operation in a varying order.

The RCL3.0 does not include any key management functionality, since this depends on the application context. It also does not contain functionality for formatting the input data (e.g. padding for the RSA algorithm). This has to be provided by the user of the RCL3.0 (i.e. usually the operating system).

6 Documentation

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

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

7 IT Product Testing

The tests performed by the composite developer can be divided into the following categories:

1. Unit Tests - individual functions are tested with specific inputs. The unit tests are performed on emulator as well as on chip, except for tests cases involving a chip reset, which are performed on emulator only,
2. Integration Tests - the user functions are tested, individually and when they are working together, for example in a user program. Integration tests include interface tests (API tests), random input tests (random tests), and functionality tests in different clock settings (HeatRun Tests),
3. System Tests - speed and memory consumption tests (including stack- and section-size testing), and
4. Countermeasure Correctness Testing - verification of the security countermeasures.

The evaluators were able to repeat the tests of the developer by sampling. Some test protocols of the tests provided by the developer were verified. In addition the evaluators performed independent tests to supplement, augment and to verify the tests performed by the developer. The tests of the evaluators comprise special tests and examination of the RCL software using open samples.

The evaluation provides evidence that the TOE provides the TOE Security Functionality as specified by the developer. The test results confirm the correct implementation of the TOE Security Functionality.

For penetration testing the evaluators took all TOE Security Functionality into consideration. Extensive penetration testing was performed to test the security mechanisms used to provide the Security Services and Security Features. The tests for the composite TOE considered the requirements to the software. Although the final ETR for Composition of the hardware platform was not available when the tests were carried out, the information was available to the evaluators, because the hardware platform has also been evaluated at T-Systems. The penetration tests considered both the side channel analysis and fault injection attacks. The test of the composite TOE comprises attacks that must be averted by the combination of the hardware platform and the IC Embedded Software as well as attacks against the software hardware platform (stack overflow).

The penetration testing was performed using the evaluators' testing environment. All configurations of the TOE being intended to be covered by the current evaluation were tested.

The penetration tests tested all SFRs.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential High was actually successful in the TOE's operational environment as defined in the RCL3.0 on RS4FC128 Version 01 Security Target ([6], [8]) provided that all measures required by the guidance are applied.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

The TOE is Renesas' Cryptographic Library running on Renesas' certified product hardware platform (RS4FC128) without any Security IC Embedded Software. The TOE is intended to be used by the secure application software (Security IC Embedded Software), which is not in scope of the evaluation, however the Security IC Embedded Software programmer is responsible for the proper use of the TOE. The hardware platform requires the implementation of the RNG on-line test software (described in [17]), which is implemented as a security functionality of the TOE. The RCL3.0 on RS4FC128 supports the development of Security IC Embedded Software.

The underlying hardware (RS4FC128) can also be delivered as embedded device (RS4FC128E). Therefore there are two names and configurations for the hardware of the TOE. However the secure boot loader software of the hardware platform can be delivered in different configurations, as described in [17].

The TOE type in question is a Security IC. The hardware platform uses state-of-the-art smart card security technologies like glue logic, shielding, anti-DPA/DFA measures, and requests further secure measures to be implemented in the software. The Renesas RCL3.0 (version 5897) on RS4FC128 Version 01 integrated circuit Product Type Code 00 and Renesas RCL3.0 (version 5897) on RS4FC128E Version 01 integrated circuit Product Type Code 01 implements security functions equipped with the secure measures. The security functionalities implemented in RCL3.0 on RS4FC128(E) fulfil the requirements of the hardware platform or fulfil a part of them and require further secure measures to the secure application software as stated in [15].

9 Results of the Evaluation

9.1 CC specific results

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 up to EAL5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

- Supporting Document – Mandatory Technical Document, The Application of CC to Integrated Circuits
- Supporting Document – Mandatory Technical Document, Application of Attack Potential to Smartcards
- Supporting Document – Guidance, Smartcard Evaluation

(see [4], AIS 25, AIS 26, AIS 37).

For RNG assessment the scheme interpretation AIS 31 was used (see [4]).

To support composite evaluations according to AIS 36 the document ETR for composite evaluation [10] was provided and approved. This document provides details of this platform evaluation that have to be considered in the course of a composite evaluation on top.

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

- All components of the EAL 5 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_DVS.2 and AVA_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance:

  Security IC Platform Protection Profile, Version 1.0, 15 June 2007,
  BSI-CC-PP-0035-2007 [7]

- for the Functionality:

  PP conformant plus product specific extensions
  Common Criteria Part 2 extended

- for the Assurance:

  Common Criteria Part 3 conformant EAL 5 augmented by ALC_DVS.2, AVA_VAN.5

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

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

9.2 Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But Cryptographic Functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context).

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
1	Cryptographic Primitive	Triple-DES in ECB, CBC, OFB	NIST SP 800-67, NIST SP 800-38A	112	No
2		Triple-DES in ECB		168	No
3		Triple-DES in CBC, OFB	NIST 800-67, NIST SP 800-38A	168	Yes
4		AES in ECB	FIPS 197, NIST SP800-38A	128, 192, 256	No
5		AES in CBC, OFB		128, 192, 256	Yes
6		RSA encryption and decryption (RSAEP, RSADP)	PKCS#1 v2.1	1024 to 1975	No
7				1976 to 2048	Yes
8		RSA signature generation and verification (RSASP1, RSAVP1)	PKCS#1 v2.1	1024 to 1975	No
9				1976 to 2048	Yes

Table 5: TOE cryptographic functionality

10 Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process.

Some security measures are partly implemented in the hardware and require additional configuration or control or measures to be implemented by the IC Dedicated Support Software or Embedded Software.

For this reason the TOE includes guidance documentation (see table 2) which contains guidelines for the developer of the IC Dedicated Support Software and Embedded Software on how to securely use the microcontroller chip and which measures have to be implemented in the software in order to fulfil the security requirements of the Security Target of the TOE.

In the course of the evaluation of the composite product or system it must be examined if the required measures have been correctly and effectively implemented by the software. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document ETR for composite evaluation [10].

11 Security Target

For the purpose of publishing, the Security Target [8] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12 Definitions

12.1 Acronyms

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CBC	Cipher Block Chaining, mode of operation for block ciphers
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ECB	Electronic Codebook Mode, mode of operation for block ciphers
ETR	Evaluation Technical Report
IC	Integrated Circuit
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
NIST	National Institute of Standards and Technologies

OFB	Output Feedback Mode, mode of operation for block ciphers
PP	Protection Profile
RNG	Random Number Generator
ROM	Read Only Memory
RSA	An algorithm for public-key encryption developed by Rivest, Shamir and Adleman
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a 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 - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

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

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 4, September 2012

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

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

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

[6] Security Target for BSI-DSZ-CC-0873-2014, Revision 7290, 27 September 2013, RCL3.0 on RS4FC128 Version 01 Security Target, Renesas Electronics Corporation (confidential document)

[7] Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007

[8] Security Target for BSI-DSZ-CC-0873-2014, Revision 7716, 17 January 2014, RCL3.0 on RS4FC128 Version 01 Security Target Public Version, Renesas Electronics Corporation (sanitised public document)

[9] Evaluation Technical Report, Version 1.00, 5 February 2014, Evaluation Technical Report BSI-DSZ-CC-0873, T-Systems GEI GmbH (confidential document)

[10] 0873-ETR for composite evaluation according to AIS 36 for Renesas Cryptographic Library 3.0 running on the RS4FC128, Version 1.00, 5 February 2014, 0873-ETR for composition, T-Systems GEI GmbH (confidential document)

[8] specifically

- AIS 20, Version 2, 15 May 2013, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 8, 12 February 2013, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 9, 21 March 2013, Evaluationsmethodologie für in Hardware Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 3, 15 May 2013, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, 8 June 2011, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, 3 September 2009, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 4, 15 May 2013, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 37, Version 3, 17 May 2010, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- AIS 38, Version 2.9, 8 June 2011, Reuse of evaluation results

[11] Generic Configuration List, Version 7420, 02 October 2013, RCL3.0 on RS4FC128 Generic Configuration List, Document Number RCL3.0 on RS4FC128-CC-ALC-0002, Renesas Electronics Corporation (confidential document)

[12] Certification Report BSI-DSZ-CC-0872-2013, 06 December 2013, Renesas RS4FC128 and RS4FC128E integrated circuits version 01, Bundesamt für Sicherheit in der Informationstechnik

[13] BSI-DSZ-CC-0872-2013 ETR for composite evaluation according to AIS 36, Version 1.00, 30 October 2013, 0872-ETR for composition, T-Systems GEI GmbH (confidential document)

[14] Option List for Smart Card Microcomputer (for RS4FC128), Version 0.2, Revision 22272, 16 November 2012, Renesas Electronics Corporation

[15] Renesas Cryptographic Library 3 (RCL3), User's Manual: Software, Renesas Secure Microcomputer RS-4E Series, Version 5897 (RCL3.0), Rev. 1.10, 25 September 2013, Renesas Electronics Corporation

[16] RS4FC128, RS4FC128E User's Manual: Hardware, Renesas Secure Microcomputer, RS-4E Series, Rev. 1.00, July 2013, Renesas Electronics Corporation

[17] RS-4E Series User Guidance Manual, Revision 1.1, September 2013, Renesas Electronics Corporation

[18] Secure Boot Loader Version 5560, User's Manual: Hardware, Renesas Secure Microcomputer RS-4E Series, Rev. 1.10, August 2013, Document Number R01US0044EJ0110, Renesas Electronics Corporation

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

Conformance Claim (Release 4 = chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

"The following Sections describe the constructs used in representing the assurance classes, families, and components."
"Each assurance class contains at least one assurance family."
"Each assurance family contains one or more assurance components."

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation

Assurance Class	Assurance Components
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

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

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

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 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 7 of this CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

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

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“Objectives

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

EAL1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

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.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. 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 8.5)

“Objectives

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

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 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises 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 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises 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 8.8)

“Objectives

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

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

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 8.9)

“Objectives

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

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A:	Security Target provided within a separate document.
Annex B:	Evaluation results regarding development and production environment

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0873-2014

Evaluation results regarding development and production environment

The IT product Renesas RCL3.0 (version 5897) on RS4FC128 Version 01 integrated circuit Product Type Code 00 and Renesas RCL3.0 (version 5897) on RS4FC128E Version 01 integrated circuit Product Type Code 01 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 5 March 2014, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.2)

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

No.	Site	Task within the evaluation
a)	Renesas Electronics Corporation 5-20-1, Jousuihon-cho, Kodaira-shi, Tokyo 187-8588, Japan	Development and customer support
b)	Renesas Electronics Europe Ltd. Dukes Meadow, Millboard Road, Bourne End, Buckinghamshire, SL8 5FH, U.K.	Provides evaluation deliverables and customer support
c)	Renesas Musashi Engineering Services Co., Ltd. 5-22-1, Jousuihon-cho, Kodaira-shi, Tokyo 187-8522, Japan	Provides customer support for built-in software and write data
d)	Renesas Electronics Corporation Naka Factory 751 Horiguchi, Hitachinaka-shi, Ibaraki-ken 312-8504, Japan	Wafer manufacturing and test site
e)	Toppan Printing Co., Ltd. 7-21-33 Nobidome, Niiza-shi, Saitama 352-0011, Japan	Preparation of masks
f)	Renesas Electronics Corporation Naka Factory 730 Horiguchi, Hitachinaka-shi, Ibaraki 312-0034, Japan	Test center

No.	Site	Task within the evaluation
g)	MTEX Matsumura Corp. 2-2-2 Kitamachi, Obanazawa-shi Yamagata 999-4231, Japan	Module Assembly
h)	Renesas Electronics Europe GmbH Karl-Hammerschmidt-Str. 42, 85609 Aschheim-Dornach, Germany	Test and development for Secure Boot Loader

d) to h) Sites from the basis security IC certification

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [8]) are fulfilled by the procedures of these sites.