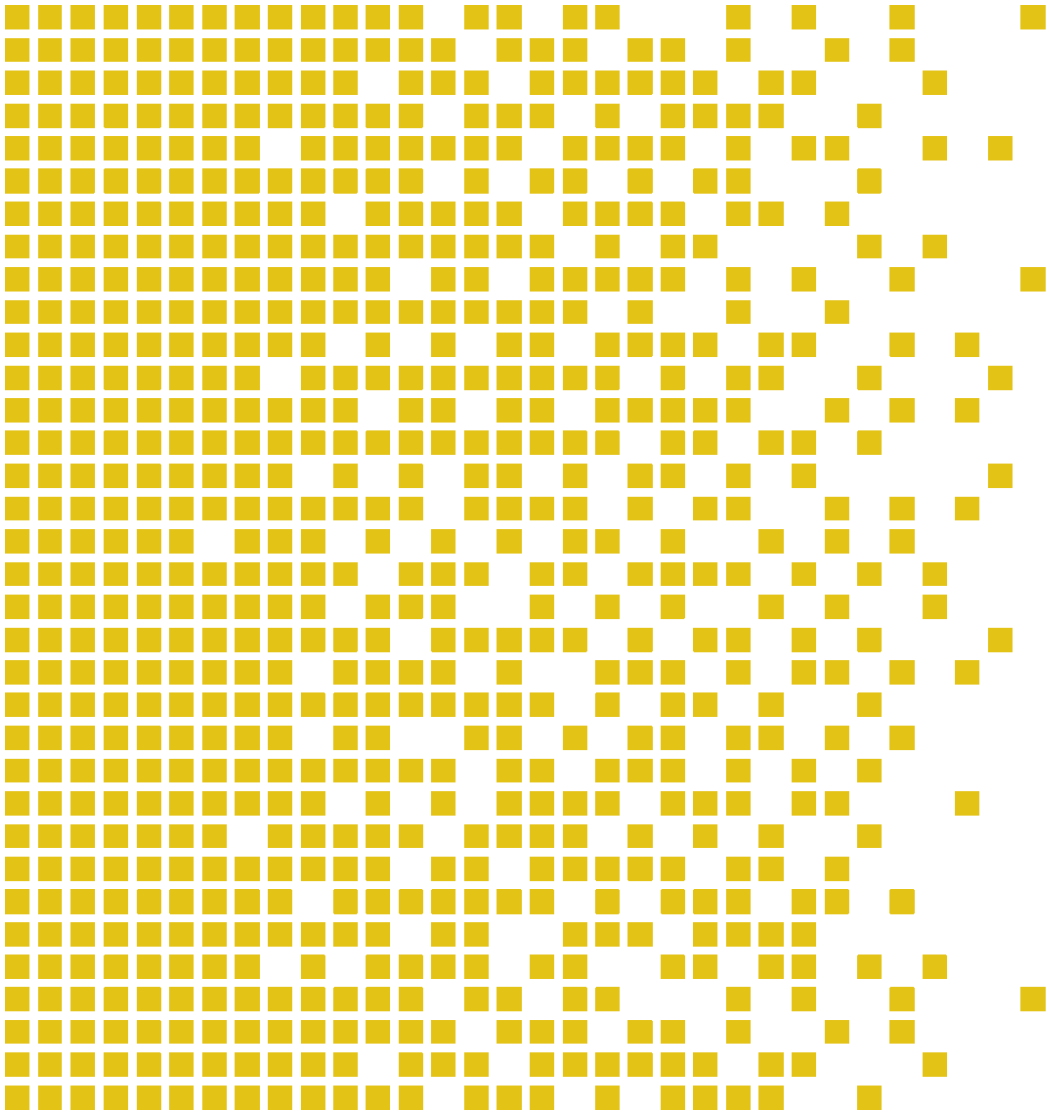
SERTIT-044 CR Certification Report

Issue 1.0 20 November 2013

SHHIC SHC1302/2907M4 with Crypto Library V1.10 and ITCOS V1.00 version HHIC2907M4



SERTIT, P.O. Box 14, N-1306 Bærum postterminal, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party. *

* Mutual Recognition under the CC recognition arrangement applies to EAL 4 but not to AVA_VAN.5 and ALC_DVS.2.

Contents

1 Certification Statement

Shanghai Huahong Integrated Circuit Co., ltd (SHHIC) SHHIC SHC1302/2907M4 with Crypto Library V1.10 and ITCOS V1.00 is a high-end dual-interface secure smart card integrated circuit suitable for banking, e-passport, social security, pay-TV and mobile payment smart card based applications.

SHHIC SHC1302/2907M4 with Crypto Library V1.10 and ITCOS V1.00 version HHIC2907M4 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and have met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL4 augmented with AVA_VAN.5 and ALC_DVS.2 for the specified Common Criteria Part 2 (ISO/IEC 15408) extended functionality in the specified environment when running on the platforms specified in Annex A. It has also met the requirements of Protection Profile BSI-PP-0035 / version 1.0 / 15-06-2007.

Author	Kjartan Jæger Kvassnes Certifier
Quality Assurance	Lars Borgos Quality Assurance
Approved	Kjell W. Bergan Head of SERTIT
Date approved	20 November 2013

2 Abbreviations

API	Application Programming Interface
ATR	Answer to reset
CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
CRC	Cyclic Redundancy Check
DEMA	Differential Electro Magnetic Analysis
DES	Data Encryption Standard
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
HO-DEMA	High-Order Differential Electro Magnetic Analysis
HO-DPA	High-Order Differential Power Analysis
OTP	One Time Programmable
POC	Point of Contact
QP	Qualified Participant
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest, Shamir, Adleman Public Key Encryption
SEMA	Simple Electro Magnetic Analysis
SERTIT	Norwegian Certification Authority for IT Security

SPA	Simple Power Analysis
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] SHHIC secure microcontroller SHC1302 / 2907M4 with crypto library V1.10 Security Target, V1.0, 2013-Aug-28.

[2] Common Criteria Part 1, CCMB-2009-07-001, Version 3.1 R3, July 2009.

[3] Common Criteria Part 2, CCMB-2009-07-002, Version 3.1 R3, July 2009.

[4] Common Criteria Part 3, CCMB-2009-07-003, Version 3.1 R3, July 2009.

[5] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2009-07-004, Version 3.1 R3, July 2009.

[7] Evaluation Technical Report Common Criteria EAL4+ Evaluation of SHHIC SHC1302/2907M4 with Crypto Library V1.10 and ITCOS V1.00, version 1.2, 8 October 2013.

[8] SHC1302/2907M4 Application Note IC Security Guide, v 1.15

[9] SHC1302/2907M4 Crypto Library User Guide, v 1.12

[10] SHC1302/2907M4 Crypto Library Check Guide, v 1.03

[11] BSI-PP-0035 / version 1.0 / 15-06-2007.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of SHHIC SHC1302/2907M4 with Crypto Library V1.10 and ITCOS V1.00 version HHIC2907M4 to the Sponsor, Shanghai Huahong Integrated Circuit Co., ltd (SHHIC), and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The version of the product evaluated was SHHIC SHC1302/2907M4 with Crypto Library V1.10 and ITCOS V1.00 and version HHIC2907M4.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Shanghai Huahong Integrated Circuit Co., ltd (SHHIC).

The TOE is a high-end dual-interface secure smart card integrated circuit suitable for (amongst others) banking, e-passport, social security, pay-TV and mobile payment applications. The TOE consists of the IC hardware and IC dedicated support software providing cryptographic functions. The hardware is based on a 32-bit CPU with volatile, non-volatile and read-only memory. The microcontroller incorporates cryptographic coprocessors for acceleration of symmetric and asymmetric encryption algorithms.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

The TOE scope is described in the ST[1], chapter 1.4.

4.4 Protection Profile Conformance

The Security Target[1] claimed conformance to the following protection profile:

BSI-PP-0035 / version 1.0 / 15-06-2007

4.5 Assurance Level

The assurance incorporated predefined evaluation assurance level EAL4+, augmented withAVA_VAN.5 and ALC_DVS.2. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

The TOE security policies are described in the ST[1], chapter 2.3.

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats which these objectives meet and security functional requirements and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

Except for FAU_SAS.1 and FCS_RNG.1 all assignments and selections are completely defined in the "Security IC Platform Protection Profile"[11]. These two exceptions are described in full detail in the ST[1], chapter 3.3

4.8 Threats Countered

All threats that are countered are described in the PP[11], chapter 3.2.

4.9 Threats Countered by the TOE's environment

There are no threats countered by the TOE's environment.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

The assumptions that apply to this TOE are all assumptions described in section 3.4 of the "Security IC Platform Protection Profile"[11].

4.12 IT Security Objectives

The security objectives that apply to this TOE are all described in section 4.1 of the "Security IC Platform Protection Profile"[11]

4.13 Non-IT Security Objectives

The security objectives for the environment are divided into two parts and are described in section chapter 4.2 and 4.3 of the "Security IC Platform Protection Profile"[11].

4.14 Security Functional Requirements

The following Security Functional Requirements are directly taken from the "Security IC Platform Protection Profile"[11]. Except for FAU_SAS.1 and FCS_RNG.1 all

assignments and selections are completely defined in the "Security IC Platform Protection Profile"[11].

- FRU_FLT.2 "Limited fault tolerance"
- FPT_FLS.1 "Failure with preservation of secure state"
- FMT_LIM.1 "Limited capabilities"
- FMT_LIM.2 "Limited availability"
- FAU_SAS.1 "Audit storage"
- FPT_PHP.3 "Resistance to physical attack"
- FDP_ITT.1 "Basic internal transfer protection"
- FDP_IFC.1 "Subset information flow control"
- FPT_ITT.1 "Basic internal TSF data transfer protection"
- FCS_RNG.1 "Quality metric for random numbers"

4.15 Security Function Policy

The TOE is a high-end dual-interface secure smart card integrated circuit suitable for (amongst others) banking, e-passport, social security, pay-TV and mobile payment applications. The TOE consists of the IC hardware and IC dedicated support software providing cryptographic functions. The hardware is based on a 32-bit CPU with volatile, non-volatile and read-only memory. The microcontroller incorporates cryptographic coprocessors for acceleration of symmetric and asymmetric encryption algorithms.

The device supports the following communication interfaces:

- ISO7816 contact interface,
- ISO14443 contactless interface
- General purpose IO (GPIO).

Also part of the TOE is documentation consisting of IC data sheet, guidance document for secure software development and guidance document for using crypto library.

The TOE has been designed to protect the integrity of its functional behaviour and protect the confidentiality and integrity of user data against physical and logical attacks.

4.16 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a

member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by the Brightsight B.V. Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR)[7] to SERTIT in 8 October 2013. SERTIT then produced this Certification Report.

4.17 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3 [4]. These classes comprise the EAL 4 assurance package augmented with AVA_VAN.5 and ALC_DVS.2.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_VAN.5	Advanced methodical vulnerability analysis

All assurance classes were found to be satisfactory and were awarded an overall "pass" verdict.

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version have been supplied, and to check that the security of the TOE has not been compromised in delivery.

5.3 Installation and Guidance Documentation

Installation procedures are described in detail in the supporting documents[8][9][10].

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Developers should follow the guidance[8][9][10] for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

An independent vulnerability analysis has been performed. The vulnerability analysis presented comprises of the following steps:

- A design and implementation review on the TOE was performed to identify weaknesses in the TOE that could potentially be exploited by attackers.
- Validation tests of security features performed in ATE are taken into account for the following vulnerability analysis.
- A vulnerability analysis based on the design and implementation review results and the validation test results of security features, was performed considering the well-known attacks from the "JIL Attack Methods for Smartcards and

Similar Devices". User guidance is also within the consideration while analysing potential vulnerabilities.
- A penetration test plan is established based on the results of the vulnerability analysis.
- Practical penetration tests are performed according the penetration test plan.

The evaluation started on the TOE of SHC1302/2907M4 with Crypto Library V1.00 and ITCOS V1.00. After the design and implementation review on the SHC1302/2907M4 with Crypto Library V1.00 and ITCOS V1.00. Several potential vulnerabilities are identified. For the three vulnerabilities from the cypto library V1.00, the developer SHHIC decided to eliminate the potential vulnerabilities by updating the software part of the TOE directly. For the other potential vulnerabilities, penetration testing plans are considered.

5.6 Developer's Tests

The developer tests consist of three parts, testing on engineering samples, testing on wafer sorting and testing on FPGA board.

- Testing on engineering samples:
  - Developer tests performed on engineering samples (cards or Dual-Inline-Package ICs).
- Testing on wafer sorting:
  - Developer tests performed on wafers.
- Testing on FPGA board:
  - Developer tests performed on FPGA board for several RSA crypto library functions.

5.7 Evaluators' Tests

The evaluator's responsibility for performing independent testing is required by the ATE_IND class. Since SHHIC's testing procedures have been found to be extensive and thorough, and SHHIC's hardware testing tools are not generally available to allow reproduction of SHHIC test cases in the test lab, the choice was made to perform the evaluator independent testing by witnessing of SHHIC's test cases, using SHHIC's tools, at the premises of SHHIC. The evaluator employs a sampling strategy to select developer tests to validate the developer's test results. The sampling strategy is as follows:

- At least one test is chosen for each SFR-enforcing subsystem
- If there are several tests mapped to a subsystem and only one test is selected to repeat, the test that tests a security function/mechanism will be the preference.

In addition to this, the evaluator has defined additional test cases, prompted by study of the developer documentation. The test stratagem is as shown below.

- Augmentation of developer testing for interfaces by varying parameters to more rigorously test the interface
- Performing positive and negative tests on selected Security Function or Security Mechanism
- Re-performing tests that use a multiple-operation ITCOS command with de-layered single-operation ITCOS commands

These tests are also performed using the developer's tools at the premises of the developer. The evaluator witnessed the whole process of the tests.

5.8 Scheme tests of the random number generator (RNG)

The Norwegian national security authority did extensive tests on the random number generator (RNG) of the chip.

The overall conclusion was that the random number generator of the chip was of satisfactory quality. There are indications of the TRNG to have a small bias, however this disappears after post-processing.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that SHHIC SHC1302/2907M4 with Crypto Library V1.10 and ITCOS V1.00 version HHIC2907M4 meet the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL4 augmentet with AVA_VAN.5 and ALC_DVS.2 for the specified Common Criteria Part 2 extended functionality and ProtectionProfile BSI-PP-0035 / version 1.0 / 15-06-2007, in the specified environment.

6.2 Recommendations

Prospective consumers of SHHIC SHC1302/2907M4 with Crypto Library V1.10 and ITCOS V1.00 version HHIC2907M4 should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above in Section 4.3 “TOE Scope” and Section 5 “Evaluation Findings”.

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

Item	Identifier	Versions
Hardware	SHC1302/2907M4 Integrated Circuit	HHIC2907M4
Software	IC Dedicated Support Software (crypto library)	1.10
	IC Dedicated Test Software and Boot Software (ITCOS)	1.00
Manuals	SHC1302/2907M4 Application Note IC Security Guide	1.15
	SHC1302/2907M4 Crypto Library User Guide	1.12
	SHC1302/2907M4 Crypto Library Check Guide	1.03

TOE Documentation

The supporting guidance documents evaluated were:

[a] SHC1302/2907M4 Application Note IC Security Guide, v 1.15

[b] SHC1302/2907M4 Crypto Library User Guide, v 1.12

[c] SHC1302/2907M4 Crypto Library Check Guide, v 1.03

Further discussion of the supporting guidance material is given in Section 5.3 "Installation and Guidance Documentation".

TOE Configuration

The configuration used for testing vas the same used for the developers tests, this is described in chapter 5.6 of this report.