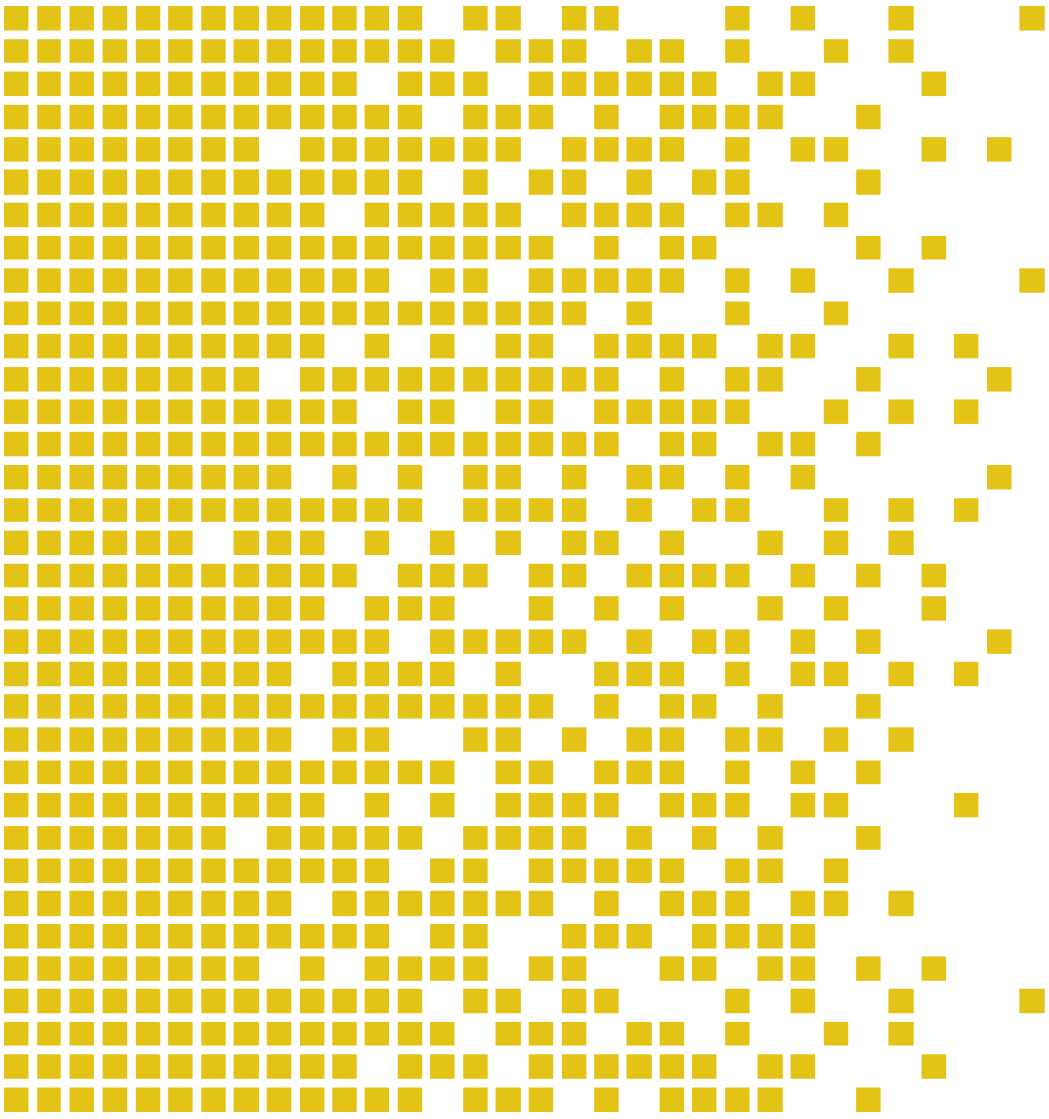
SERTIT-074 CR Certification Report

Issue 2.0 08 June 2016

THD88/M2064 Secure Microcontroller with Crypto Library



SERTIT, Postboks 814, 1306 Sandvika, 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.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of CCRA July 2nd 2014. The recognition under CCRA is limited to cPP related assurance packages or EAL 2 and ALC_FLR CC part 3 components.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (SOGIS MRA)

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

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.

The recognition under SOGIS MRA is for components up to EAL 4.

Contents

1 Certification Statement

Beijing Tongfang Microelectronics Co., Ltd. THD88/M2064 Secure Microcontroller with Crypto Library is a high-end dual-interface secure smart card integrated circuit suitable for ID cards, Banking cards, e-Passport applications and the like.

THD88/M2064 Secure Microcontroller with Crypto Library has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL 4 augmented with AVA_VAN.5, ATE_DPT.2 and ALC_DVS.2 (see chapter 5) 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-CC-PP-0084-2014 V1.0.

Author	Arne Høye Rage Certifier
Quality Assurance	Lars Borgos Quality Assurance
Approved	Kristian Steinfeldt Bae Head of SERTIT
Date approved	08 June 2016

Changes to document:

Version	Date	Description
2.0	08 June 2016	Added text " The recognition under SOGIS MRA is for components up to EAL 4." in SOGIS MRA text box on page 2. Updated document version, date and signature table. Minor editorial corrections.

2 Abbreviations

API	Application Programming Interface
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
DEMA	Differential Electro Magnetic Analysis
DES	Data Encryption Standard
DPA	Differential Fault Analysis
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
EMFI	Electro-Magnetic Fault Injection
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
FBBI	Forward-Body Bias Injection
IC	Integrated Circuit
OSP	Organizational Security Policy
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest, Shamir, Adleman Public Key Encryption
SERTIT	Norwegian Certification Authority for IT Security
SEMA	Simple Electro Magnetic Analysis
SFR	Security Functional Requirements
SPA	Simple Power Analysis
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] Security Target, Beijing Tongfang Microelectronics Co., Ltd., THD88/M2064 Secure Microcontroller with Crypto Library Security Target, Version 1.1, November 2015.

[2] Common Criteria Part 1, CCMB-2012-09-001, Version 3.1 R4, September 2012.

[3] Common Criteria Part 2, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[4] Common Criteria Part 3, CCMB-2012-09-003, Version 3.1 R4, September 2012.

[5] The Norwegian Certification Scheme, SD001E, Version 9.0, 2 April 2013.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.

[7] JIL Attack Methods for Smartcards and Similar Devices, Version 2.2, January 2013.

[8] JIL Application of Application Attack Potential to Smart Cards, Version 2.9, May 2013.

[9] AIS20/31 A proposal for Functionality classes for random number generators, Version 2.0, 18 September 2011.

[10] Evaluation Technical Report of THD88/M2064 Secure Microcontroller with Crypto Library, 15-RPT-348 Version 1.1, 20 November 2015.

[11] THD88/M2064 AGD Operational Guidance, Version 0.8, 8 October 2015.

[12] THD88/M2064 Secure Microcontroller with Crypto Library Secure Microcontroller Security Guideline, Version 0.7, 8 October 2015.

[13] THD88/M2064 Secure Microcontroller with Crypto Library Preparative Guidance, Version 0.4, 7 October 2015.

[14] THD88/M2064 Secure Microcontroller with Crypto Library International Cryptographic Algorithm API, Version 1.6, October 2015.

[15] Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, Version 1.0, January 2014.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of THD88/M2064 Secure Microcontroller with Crypto Library to the Sponsor, Beijing Tongfang Microelectronics Co., Ltd., 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 THD88/M2064 Secure Microcontroller with Crypto Library.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Tongfang Microelectronics Company.

The TOE is suitable for instance to support ID cards, Banking cards, e-Passport applications and the like. It consists of a dual-interface THD88 Integrated Circuit with a DES/RSA coprocessor and a True Random Number Generator (AIS20/31 class PTG.2), a crypto library for DES and RSA and IC Dedicated Boot Software.

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 Security Target[1], chapter 1.3.

4.4 Protection Profile Conformance

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

BSI-CC-PP-0084-2014 V1.0

4.5 Assurance Level

The Security Target[1] specified the assurance requirements for the evaluation. The assurance incorporated predefined evaluation assurance level EAL 4, augmented by AVA_VAN.5, ATE_DPT.2 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]. The assurance components with full names are listed in chapter 5.

4.6 Security Policy

The TOE security policies are detailed in Security Target[1] , chapter 3.3.

4.7 Security Claims

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

The following SFR's are defined in the Protection Profile[15]:FCS_RNG.1, FMT_LIM.1, FMT_LIM.2, FAU_SAS.1, FDP_SDC.1.

4.8 Threats Countered

All threats that are countered are described in the Security Target[1], 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 are described that are not countered.

4.11 Environmental Assumptions and Dependencies

The assumptions that apply to this TOE are described in the Security Target[1], chapter 3.4.

4.12 IT Security Objectives

The security objectives that apply to this TOE are described in the Security Target[1], chapter 4.1.

4.13 Non-IT Security Objectives

The security objectives for the environment are described in the Security Target[1], chapter 4.2 and 4.3.

4.14 Security Functional Requirements

The following Security Functional Requirements are directly taken from the Protection Profile[15]. Except for FAU_SAS.1, FDP_SDC.1, FDP_SDI.2, FCS_RNG.1 and FCS_COP.1 all assignments and selections are completely defined in the Protection Profile[15].

Security functional requirement	Title
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"
FDP_SDC.1	"Stored data confidentiality"
FDP_SDI.2	"Stored data integrity monitoring and action"
FCS_RNG.1[PTG.2]	"Quality metric for random numbers"
FCS_COP.1[DES]	"Cryptographic operation - TDES"
FCS_COP.1[RSA]	"Cryptographic operation - RSA"

4.15 Security Function Policy

The TOE is a secure microcontroller with crypto library suitable for instance to support ID cards, Banking cards, e-Passport applications and the like.

The TOE consists of hardware and IC dedicated software. The hardware is based on a 32-bit CPU with ROM (Non-Volatile Read-Only Memory), EEPROM (Non-volatile Programmable Memory) and RAM (Volatile Memory). The hardware of the TOE also incorporates communication peripherals and cryptographic coprocessors for execution and acceleration of symmetric and asymmetric cryptographic algorithms. The IC dedicated software consists of boot code and a library of cryptographic services.

The TOE supports the following communication interfaces:

- ISO/IEC 7816 contact interface.
- ISO/IEC 14443 contactless interface

The TOE is delivered to a composite product manufacturer. The security IC embedded software is developed by the composite product manufacturer. The security IC embedded software is sent to Tongfang Microelectronics Company to be implemented

in ROM and delivered back to the composite product manufacturer together with the TOE. The security IC embedded software is not part of the TOE.

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 Mutual Recognition Agreement Of Information Technology Security Evaluation Certificates (SOGIS MRA). The evaluation was conducted in accordance with the terms of these arrangements.

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]. Interpretations[7][8][9] are used.

SERTIT monitored the evaluation which was carried out by Brightsight B.V. as Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[10] to SERTIT on 20 November 2015. As a result 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 EAL4 assurance package augmented with AVA_VAN.5, ATE_DPT.2 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 life-cycle model
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: security enforcing modules
	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[10] 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 of its constituent components has been supplied, and to check that the security of the TOE has not been compromised in delivery.

The delivery procedure is described in the supporting document[13].

5.3 Installation and Guidance Documentation

Installation procedures are described in detail in the supporting document[13].

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Security IC Embedded Software shall follow the guidance documentation[11][12][13] for the TOE in order to ensure that the TOE is operated 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 was done, consisting of the following steps:

- A design and implementation review on the TOE was done to identify weaknesses in the TOE that could potentially be exploited by attackers. A code review of the crypto library and boot code was also executed.
- Validation tests of security features performed in the ATE class 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"[7]. User guidance is also taken into 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.

5.6 Developer's Tests

The developer tests consist of four parts; 1) testing on engineering samples, 2) testing on wafers, 3) testing on simulation tools and 4) testing on an emulation board (FPGA).

- Testing on engineering sample:

  Developer tests performed on engineering samples (cards or Dual-In-Line-Package ICs)

- Testing on wafer:

  Developer tests performed on wafers

- Testing on simulation tools:

  Developer tests were done on simulation tools in the chip development environment, which were used to verify the logical functions.

- Testing on the emulation board:

  Developer tests were done on an emulation board (FPGA), mainly for the Crypto library.

5.7 Evaluators' Tests

The evaluator's responsibility for independent testing is required by the ATE_IND class. Since developer's testing procedures were found to be extensive and thorough, and developer's hardware testing tools are not generally available to allow reproduction of developer test cases in the evaluator's test lab, the choice was made to perform the evaluator independent testing by witnessing of the developer's test cases, using the developer's tools, at the premises of the developer. The evaluator used 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, the test(s) that verify security functions/mechanism will be preferred.

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

- Augmentation of developer testing for interfaces by varying parameters in order to more rigorously test the interface
- Performing positive and negative tests on selected Security Functions or Security Mechanisms.

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.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[10], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that THD88/M2064 Secure Microcontroller with Crypto Library meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 4 augmented with AVA_VAN.5, ATE_DPT.2 and ALC_DVS.2 for the specified Common Criteria Part 2 extended functionality and Protection Profile BSI-CC-PP-0084-2014 V1.0, in the specified environment.

6.2 Recommendations

Prospective consumers of THD88/M2064 Secure Microcontroller with Crypto Library 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 under 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.

The above "Evaluation Findings" include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

Type	Name	Version	Package
Hardware	THD88	0.1	module
Software	Crypto library	1.2	software library in ROM
	Boot code	1.0	boot code in ROM
Manual	THD88/M2064 AGD Operational Guidance[11]	0.8	document
	THD88/M2064 Secure Microcontroller with Crypto Library Preparative Guidance[13]	0.4	document
	THD88/M2064 Secure Microcontroller Security Guidelines[12]	0.7	document

TOE Documentation

The supporting guidance documents evaluated were:

[a] THD88/M2064 AGD Operational Guidance, Version 0.8, 8 October 2015[11]

[b] THD88/M2064 Secure Microcontroller with Crypto Library Preparative Guidance, Version 0.4, 7 October 2015[13]

[c] THD88/M2064 Secure Microcontroller with Crypto Library Secure Microcontroller Security Guideline, Version 0.7, 8 October 2015[12]

TOE Configuration

The TOE configuration used for testing was the same used for developer tests, this is described in chapter 5.6 of this report.