Reference: 2023-33-INF-4571- v1
Target: Limitada al expediente
Date: 15.07.2025

Created by: I003
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2023-33**
TOE	**THD89 Secure Microcontroller version 1.0**
Applicant	**911100007334588792 - Tongxin Microelectronics Co., Ltd.**
References	

[EXT-8805] Certification request

[EXT-9905] Evaluation Technical Report

Certification report of the product THD89 Secure Microcontroller version 1.0, as requested in [EXT-8805] dated 19/09/2023, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-9550] received on 11/04/2025.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product THD89 Secure Microcontroller version 1.0.

The TOE is a secure microcontroller with crypto library suitable to support ID cards, banking cards, ePassport applications, etc.

Developer/manufacturer: Tongxin Microelectronics Co., Ltd.

Sponsor: Tongxin Microelectronics Co., Ltd..

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Nombre Laboratorio.

Protection Profile: Security IC Platform Protection Profile, BSI-CC-PP-0084-2014 (version 1.0, 13.01.2014).

Evaluation Level: Common Criteria 3.1 R5 EAL6 + ASE_TSS.2 + ALC_FLR.1.

Evaluation end date: 09/06/2025

Expiration Date[1]: 16/07/2030

All the assurance components required by the evaluation level EAL6 (augmented with ASE_TSS.2 + ALC_FLR.1,) have been assigned a “PASS” verdict. Consequently, the laboratory Applus Laboratories assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL6 + ASE_TSS.2 + ALC_FLR.1, as defined by the Common Criteria 3.1 R5 and the CEM 3.1 R5.

Considering the obtained evidence during the instruction of the certification request of the product THD89 Secure Microcontroller version 1.0, a positive resolution is proposed.

TOE SUMMARY

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), NVM (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.

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL6 and the evidence required by the additional component ASE_TSS.2 + ALC_FLR.1 to the table, according to Common Criteria v3.1 R5.

Security assurance requirements	Titles
Class ADV: Development	
ADV_ARC.1	Architectural design
ADV_FSP.5	Functional specification
ADV_IMP.2	Implementation representation
ADV_INT.3	TSF internals
ADV_SPM.1	Security policy modelling
ADV_TDS.5	TOE design
Class AGD: Guidance documents	
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative user guidance
Class ALC: Life-cycle support	
ALC_CMC.5	CM capabilities
ALC_CMS.5	CM scope
ALC_DEL.1	Delivery
ALC_DVS.2	Development security
ALC_FLR.1	Basic flaw remediation
ALC_LCD.1	Life-cycle definition
ALC_TAT.3	Tools and techniques
Class ASE: 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.2	TOE summary specification
Class ATE: Tests	
ATE_COV.3	Coverage
ATE_DPT.3	Depth
ATE_FUN.2	Functional testing
ATE_IND.2	Independent testing
Class AVA: Vulnerability analysis	
AVA_VAN.5	Vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R5:

SECURITY FUNCTIONAL REQUIREMENTS
FRU_FLT.2
FPT_FLS.1
FMT_LIM.1
FMT_LIM.2
FAU_SAS.1
FPT_PHP.3
FDP_ITT.1
FPT_ITT.1
FDP_IFC.1
FDP_SDC.1
FDP_SDI.2
FCS_RNG.1[PTG.2]
FCS_COP.1[TDES]
FCS_COP.1[AES]
FCS_COP.1[RSA-CRT]
FCS_COP.1[ECC]

IDENTIFICATION

Product: THD89 Secure Microcontroller version 1.0.

Security Target: THD89 Secure Microcontroller version 1.0 Security Target, version 2.2 (Nov. 2024).

Protection Profile: Security IC Platform Protection Profile, BSI-CC-PP-0084-2014 (version 1.0, 13.01.2014).

Evaluation Level: Common Criteria 3.1 R5 EAL6 + ASE_TSS.2 + ALC_FLR.1.

SECURITY POLICIES

The use of the product THD89 Secure Microcontroller version 1.0 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target, section 3.3 (“Organisational Security Policies”).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

The detail of these assumptions is documented in the Security Target, section 3.4 (“Assumptions”).

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product THD89 Secure Microcontroller version 1.0, although the agents implementing attacks have the attack potential according to the High of EAL6 + ASE_TSS.2 + ALC_FLR.1 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are those defined in the Security Target, section 3.2 (“Threats”).

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are those defined in the Protection Profile and they are documented in the Security Target, section 4.3 (“Security Objectives for the operational Environment”).

ARCHITECTURE

LOGICAL ARCHITECTURE

The TOE provides ROM for executing the boot code and crypto library code, NVM for the code and data access, and RAM for the temporary data access.

The Memory management unit is performed by the AHBMMU, and it also performs the access control of boot mode, test mode and normal mode.

There are four communication interfaces available, including ISO/IEC 14443 contactless interface, ISO/IEC 7816 contact interface, SPI and I2C interfaces.

The TOE provides the system control functions to handle the reset, clock, interrupt signals, etc.

The TOE provides the test circuitry to perform the TOE testing under the test mode.

The TOE provides the timers for the security IC embedded software to abort irregular executions of the program.

The TOE provides power management functionality under boot mode, test mode, and normal mode, also contact and contactless interfaces.

The TOE provides strong security functionalities against malfunction, including the environmental sensors to monitor if environmental conditions are within the specified range, the abnormality check of TRNG to verify the quality of the generated random data, also the integrity to monitor if the data is manipulated.

The TOE provides strong security functionalities against leakage, including memory encryption and bus masking, 32bit secure core random branch insertion to obscures the cycle timing of code by inserting branch to self-instruction, and random OSC clock jitter to configure the oscillator frequency to a random value for each cycle.

The TOE provides strong security functionalities against physical manipulation and probing, including the dedicated shielding techniques, data integrity check for verifying the integrity of the data, also the memory and bus encryption.

The TOE provides strong security functionalities against abuse of functionality and identification by the means of test access control mechanism. It is implemented by a combination with hardware fuse and software access control mechanism.

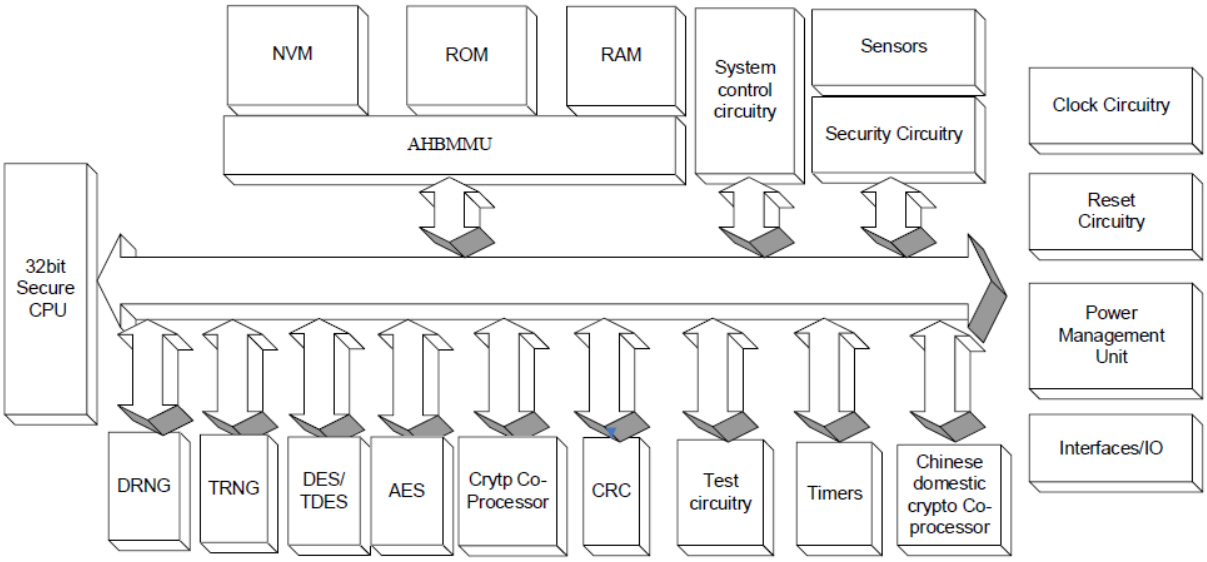
The TOE provides a true random number generator, which is accessible by the crypto library. The true random number generator is composed of entropy sources, self-test circuit and post-processing circuit. The self-test circuit includes the total failure test and online test. The total failure test is performed on the entropy source. The on line testing is performed on the raw random number sequence, aiming to prevent malfunctioning. The true random number also fulfils the AIS20/31 PTG.2 level.

The TOE provides the following cryptographic services to the Security IC embedded software:

- TDES
- RSA-CRT
- AES
- ECC

PHYSICAL ARCHITECTURE

The main functional blocks of the TOE hardware are depicted below.



The hardware of the TOE has the following components:

- 32-bit secure CPU
- NVM
- ROM
- RAM
- AHBMMU
- Interfaces I/O
  - ISO/IEC 14443 contactless interface
  - ISO/IEC 7816 contact interface
  - SPI interface
  - I2C interface
- True Random Number Generator
- Deterministic Random Number Generator
- DES/TDES Co-Processor
- AES Co-Processor
- Hardware Crypto Co-Processor for RSA-CRT and ECC support
- System control circuitry
- Test circuitry
- Timers
- Security Circuitry
- Sensors
  - Voltage sensor
  - Glitch sensor
  - Frequency sensor
  - High frequency filter
  - Temperature sensor

  - Light sensor
- Power Management Circuitry
- Clock circuitry
- Reset circuitry

The AHBMMU is a bus component which also provides user controllable bus masking.

The Deterministic Random Number Generator hardware component is used internally by the TOE. However, the service provided to the user is not under the scope of the evaluation.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- THD89 Secure Microcontroller version 1.0 Operational guidance, versión 1.7.
- THD89 Secure Microcontroller version 1.0 Preparative Guidance, versión 2.4.
- THD89 Secure Microcontroller version 1.0 Cryptographic Algorithm API, version 2.2.
- THD89 Secure Microcontroller version 1.0 Security Guideline, versión 1.8.

PRODUCT TESTING

The developer has executed tests for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.

During the evaluation process each unit test has been verified, checking that the security functionality that covers has been identified and that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the results obtained during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluator has applied sampling strategy and has concluded that the information is complete and coherent enough to reproduce tests and identify the functionality tested. Through the tests performed by the Laboratory, it is concluded that 30% of the developer tests were covered.

In addition, the lab has devised tests of the security functions of the product verifying that the results obtained are consistent with the results obtained by the developer.

It has been checked that the results obtained conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that

this variation does not represent any security problem or a decrease in the functional capacity of the product. Through the tests performed by the Laboratory it is concluded that 87,5% of the SFRs and 70% of the TSFI groups defined in the Functional Specification are covered.

PENETRATION TESTING

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment, the evaluation team has devised vulnerability analysis and attack scenarios for penetration testing according to JIL supporting documents [JIL-ATTPOT] and [JIL-ARC]. Within these activities, all aspects of the security architecture which were not covered by functional testing have been considered.

No attack scenario with the attack potential high according to Common Criteria v3.1 R5 has been successful in the TOE's operational environment as defined in the security target when all security measures required by the developer are applied.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product THD89 Secure Microcontroller version 1.0 it is necessary the disposition of the following software components:

- THD89 HW module.
- Crypto Library.
- Boot code.
- Header file.

Among all the possibilities offered by these software and hardware requirements, the configuration selected for the evaluation is the following:

Type	Name	Version	Package
Hardware	THD89	1.0	Module
Software	Crypto Library	1.01	Software library in ROM
	CryptoECCSec library	1.20	Software library in NVM
	Boot code	1.0	Boot code in ROM
	Header file	0.2	cryptolib.h

EVALUATION RESULTS

The product THD89 Secure Microcontroller version 1.0 has been evaluated against the Security Target THD89 Secure Microcontroller version 1.0 Security Target, version 2.2 (Nov. 2024).

All the assurance components required by the evaluation level EAL6 + ASE_TSS.2 + ALC_FLR.1 have been assigned a "PASS" verdict. Consequently, the laboratory Applus Laboratories assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL6 + ASE_TSS.2 + ALC_FLR.1, as defined by the Common Criteria 3.1 R5 and the CEM 3.1 R5.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

The evaluation team makes the following security recommendations:

- To follow the security guidance's of the TOE strictly.
- To keep the TOE under personal control and set all other security measures available from the environment.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidence during the instruction of the certification request of the product THD89 Secure Microcontroller version 1.0, a positive resolution is proposed.

The CCN Certification Body strongly recommends to the TOE consumer to strictly follow the security recommendations that can be found on guidance documents, taking special care of those included in document THD89 Secure Microcontroller version 1.0 Security Guideline, version 1.8, as well as to observe the operational environment requirements and assumptions defined in the applicable Security Target. The scope of the certificate only covers those product configurations that implement all security recommendations defined in THD89 Secure Microcontroller version 1.0 Security Guideline, version 1.8; otherwise, the certificate is not applicable.

The TOE consumer should also observe the application notes defined in the applicable Security Target, especially those related to the cryptographic mechanisms.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[JIL-ATTPOT] Application of Attack Potential to Smartcards. Joint Interpretation Library. Version 3.2. November 2022. Joint Interpretation Library.

[JIL-ARC] Security Architecture requirements (ADV_ARC) for smart cards, and similar devices extended to Secure Sub-Systems in SoC, version 2.1. July 2021. Joint Interpretation Library.

[ST] THD89 Secure Microcontroller version 1.0 Security Target, version 2.2 (Nov. 2024).

[ST-Lite] THD89 Secure Microcontroller version 1.0 Security Target Lite, version 1.0 (Apr. 2025).

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

Along with this certification report, the complete security target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

- THD89 Secure Microcontroller version 1.0 Security Target, version 2.2 (Nov. 2024).

The public version of this document constitutes the ST Lite. The ST Lite has also been reviewed for the needs of publication according to [CCDB-2006-04-004], and it is published along with this certification report in the Certification Body and CCRA websites. The ST Lite identifier is:

- THD89 Secure Microcontroller version 1.0 Security Target Lite, version 1.0 (Apr. 2025).

ETR FOR COMPOSITION IDENTIFICATION

The evaluation activities carried out in this certification dossier have been summarized in an Evaluation Technical Report for composite evaluation (ETR_COMP). This ETR_COMP has been validated by this Certification Body. The reference of the ETR_COMP is:

- **Report name**: ETR for composite evaluation. THD89 Secure Microcontroller version 1.0.
- **Report ID**: CCETMC002R1-ETRfC-M1.
- **Version**: M1.
- **Issue Date**: 03/06/2025.
- **SHA256**: 8a571e7d729fd30468db81838970a69025e26a7ca47ebdaed7778f6ed578aca9.
- **Issuing ITSEF**: Applus Laboratories.

The ETR_COMP report constitutes an evaluation evidence, therefore according to article 25 of Presidential Order PRE/2740/2007 which regulates the CCN Certification Body, written authorization must be requested by Applus Laboratories to the Certification Body to share any information of this certification dossier with third parties.

It is expected that if the applicant Tongxin Microelectronics Co., Ltd. is willing to share the ETR_COMP report with any third party, they may contact Applus Laboratories to perform an authorization request to the CCN Certification Body to distribute this report.

RECOGNITION AGREEMENTS

In order to avoid multiple certifications 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.

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 SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

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. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

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

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of

certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

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.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC_FLR.