GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

organismo de certificación OC-CCN centro criptológico nacional

Reference: 2024-6-INF-4742- v1
Target: Limitada al expediente
Date: 12.02.2026

Created by: I008
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2024-6**
TOE	**THC80F480C/384C/340C/280C/256C/228C/176C/150C Secure Microcontroller Version 1.0**
Applicant	**911100007334588792 - Tongxin Microelectronics Co., Ltd.**

References

[EXT-8987] 2024-03-06_2024-06_solicitud_certificacion

[EXT-9976] 2026-01-15_2024-06_ETR_M1

Certification report of the product THC80F480C/384C/340C/280C/256C/228C/176C/150C Secure Microcontroller Version 1.0, as requested in [EXT-8987] dated 06/03/2024, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-9976] received on 15/01/2026.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product THC80F480C/384C/340C/280C/256C/228C/176C/150C Secure Microcontroller Version 1.0.

The TOE is a secure Microcontroller is dedicated to applications such as for mobile phones (GSM SIM cards) etc.

The TOE consists of hardware. The hardware is based on a 32-bit secure CPU with NVM (Nonvolatile Programmable Memory) and RAM (Volatile Memory). The hardware of the TOE also incorporates communication peripherals and true random number generator.

Developer/manufacturer: Tongxin Microelectronics Co., Ltd.

Sponsor: Tongxin Microelectronics Co., Ltd..

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

ITSEF: Applus Laboratories.

Protection Profile: N/A

Evaluation Level: Common Criteria v3.1, Release 5, EAL4 + AVA_VAN.4 and ALC_DVS.2.

Evaluation end date: 21/01/2026

Expiration Date[1]: 13/02/2031

All the assurance components required by the evaluation level EAL4 (augmented with AVA_VAN.4 + ALC_DVS.2) 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 EAL4 + AVA_VAN.4 + ALC_DVS.2, as defined by the Common Criteria v3.1, Release 5 and the CEM v3.1, Revision 5.

Considering the obtained evidences during the instruction of the certification request of the product THC80F480C/384C/340C/280C/256C/228C/176C/150C Secure Microcontroller Version 1.0, a positive resolution is proposed.

[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.

TOE SUMMARY

The TOE is a secure Microcontroller is dedicated to applications such as for mobile phones (GSM SIM cards) etc.

The TOE consists of hardware. The hardware is based on a 32-bit secure CPU with NVM (Non-volatile Programmable Memory) and RAM (Volatile Memory). The hardware of the TOE also incorporates communication peripherals and true random number generator.

The TOE supports the following communication interfaces:

- ISO/IEC 7816 contact interface.
- I2C interface

The TOE has been designed to provide a platform for Security IC Embedded Software which ensures that the critical user data of the Composite TOE are stored and processed in a secure way. To this end the TOE has the following security features:

- True Random Number Generator
- Protection against power analysis
- Protection against physical attacks
- Protection against perturbation attacks

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL4 and the evidences required by the additional component AVA_VAN.4 + ALC_DVS.2 to the table, according to Common Criteria v3.1, Release 5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
ADV	ADV_ARC.1
	ADV_FSP.4
	ADV_IMP.1
	ADV_TDS.3

AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.4
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.2
	ALC_LCD.1
	ALC_TAT.1
ATE	ATE_COV.1
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.4

SECURITY FUNCTIONAL REQUIREMENTS

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

SECURITY FUNCTIONAL REQUIREMENT
FRU_FLT.2
FPT_FLS.1
FMT_LIM.1
FMT_LIM.2
FAU_SAS.1
FDP_SDC.1
FPT_PHP.3
FDP_ITT.1
FPT_ITT.1
FDP_IFC.1
FCS_RNG.1[PTG.2]

IDENTIFICATION

Product: THC80F480C/384C/340C/280C/256C/228C/176C/150C Secure Microcontroller Version 1.0

Security Target: [ST] ASE EAL4+ for TMC THC80F480C/384C/340C/280C/256C/228C/176C/150C, version 1.4, Aug. 2025.

Protection Profile: N/A.

Evaluation Level: Common Criteria v3.1, Release 5, EAL4 + AVA_VAN.4 and ALC_DVS.2.

SECURITY POLICIES

The use of the product THC80F480C/384C/340C/280C/256C/228C/176C/150C 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 ("Organizational 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 THC80F480C/384C/340C/280C/256C/228C/176C/150C Secure Microcontroller Version 1.0, although the agents implementing attacks have the attack potential according to the Moderate of EAL4 + AVA_VAN.4 + ALC_DVS.2 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 distinguishes three modes:

1. Test mode
2. ENG mode
3. Normal mode

Test mode is also not available for the Security IC embedded software. It is utilized to perform the TOE testing before the TOE is delivered to the end user. Test mode is strictly protected by a combination of hardware and software security features.

ENG mode is used for reading SN information for engineering analysis.

Normal mode is utilized for the end user, Security IC embedded software can be executed under this mode. Normal mode cannot switch back to and test mode.

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

There are two communication interfaces available, including ISO/IEC 7816 contact interface, and I2C interface.

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

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

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, bus masking.

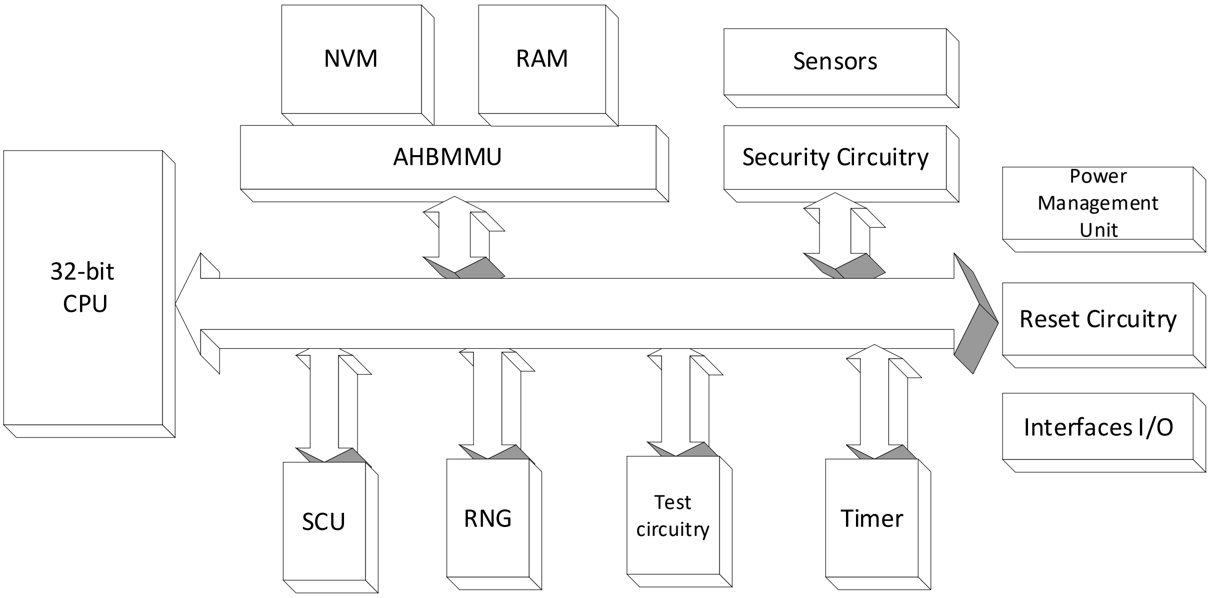
The TOE provides strong security functionalities against physical manipulation and probing, including the dedicated shielding techniques and the memory and bus encryption.

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 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.

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 core CPU
- NVM
- RAM
- AHBMMU
- Interfaces I/O
    - ISO/IEC 7816 contact interface
    - I2C interface

- True Random Number Generator
- SCU
- Test circuitry
- Timers
- Security Circuitry
- Sensors
    - Voltage sensor
    - Glitch sensor
    - Frequency sensor
    - Temperature sensor
    - Light sensor
- Power Management Unit
- Reset circuitry

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

DOCUMENTS

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

- ASE EAL4+ for TMC THC80F480C_384C_340C_280C_256C_228C_176C_150C lite, version 0.4.
- AGD_OPE OG EAL4+ for TMC THC80F480C_384C_340C_280C_256C_228C_176C_150C, version 0.7.
- AGD_OPE SG EAL4+ for TMC THC80F480C_384C_340C_280C_256C_228C_176C_150C version, 1.9.
- AGD_PRE EAL4+ for TMC THC80F480C_384C_340C_280C_256C_228C_176C_150C, version 1.1.

PRODUCT TESTING

The developer has executed test 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 it has been verified each unit test checking that the security functionality that covers is been identified and also 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 obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluator extracted a subset of the developer's tests, and extending some of them by modifying their parameters to verify that the result is still successful.

It has been checked that the obtained results 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 neither represents any security problem nor a decrease in the functional capacity of the product.

Through the tests performed by the laboratory it is concluded that 72.73% of the SFRs and 61.04% of the TSFIs defined in the Functional Specification have been tested.

PENETRATION TESTING

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

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 Moderate has been successful in the TOE's operational environment as defined in the security target when all security measures required by the developer in the security guidance defined in DOCUMENTS section are applied.

EVALUATED CONFIGURATION

The TOE consists of the following components that are delivered to the composite product manufacturer:

Type	Name	Version	Package	Format	Delivery method	Memory Size(NVM)	Hash value
Hardware	THC80F480C	1.0	Module	Module	Courier delivery	480KB	-
	THC80F384C	1.0	Module	Module	Courier delivery	384KB	-
	THC80F340C	1.0	Module	Module	Courier delivery	340KB	-

	THC80F280C	1.0	Module	Module	Courier delivery	280KB	-
	THC80F256C	1.0	Module	Module	Courier delivery	256KB	-
	THC80F228C	1.0	Module	Module	Courier delivery	228KB	-
	THC80F176C	1.0	Module	Module	Courier delivery	176KB	-
	THC80F150C	1.0	Module	Module	Courier delivery	150KB	-

Note: The hardware modules are the same design, the difference between them is due to the factory configuration of the corresponding registers, which cannot be written or read by users and cannot be altered afterward.

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

Type	Name	Version	Package	Memory Size(NVM)
Hardware	THC80F480C	1.0	Module	480KB

EVALUATION RESULTS

The product THC80F480C/384C/340C/280C/256C/228C/176C/150C Secure Microcontroller Version 1.0 has been evaluated against the Security Target [ST] ASE EAL4+ for TMC THC80F480C/384C/340C/280C/256C/228C/176C/150C, version 1.4, Aug. 2025.

All the assurance components required by the evaluation level EAL4 + AVA_VAN.4 + ALC_DVS.2 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 EAL4 + AVA_VAN.4 + ALC_DVS.2, 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.

- 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 evidences during the instruction of the certification request of the product THC80F480C/384C/340C/280C/256C/228C/176C/150C Secure Microcontroller Version 1.0, a positive resolution is proposed.

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.

SECURITY TARGET / SECURITY TARGET LITE

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:

- [ST] ASE EAL4+ for TMC THC80F480C/384C/340C/280C/256C/228C/176C/150C, version 1.4, Aug. 2025.

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:

- [ST_lite] ASE EAL4+ for TMC THC80F480C/384C/340C/280C/256C/ 228C/176C/150C Lite, version 0.4, Aug. 2025.

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.

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.