Reference: 2021-1-INF-4210- v2
Target: Pública
Date: 08.02.2024

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

CERTIFICATION REPORT

Dossier #	**2021-1**
TOE	**THN31 Secure Element version 1.0**
Applicant	**91110108MA01HQR628 - Beijing TsingTeng MicroSystem Co.,Ltd.**

References

[EXT-6488] Certification Request

[EXT-8747] Evaluation Technical Report (1/2)

[EXT-8748] Evaluation Technical Report (2/2)

Certification report of the product THN31 Secure Element version 1.0, as requested in [EXT-6488] dated 19/01/2021, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-8747 and EXT-8748] received on 03/10/2023.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product THN31 Secure Element version 1.0.

The TOE is a secure element with two crypto libraries suitable to support embedded SE, embedded SIM applications, etc.

Developer/manufacturer: Beijing TsingTeng MicroSystem Co.,Ltd.

Sponsor: Beijing TsingTeng MicroSystem 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 EAL5 + ALC_DVS.2 + AVA_VAN.5.

Evaluation end date: 15/11/2023.

Expiration Date[1]: 06/01/2029.

All the assurance components required by the evaluation level EAL5 (augmented with ALC_DVS.2 + AVA_VAN.5) 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 EAL5 + ALC_DVS.2 + AVA_VAN.5, as defined by the Common Criteria 3.1 R5 and the CEM 3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product THN31 Secure Element 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 secure 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

[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.

cryptographic algorithms. The IC dedicated software consists of boot code and two libraries of cryptographic services.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL5 and the evidences required by the additional component ALC_DVS.2 + AVA_VAN.5, according to Common Criteria v3.1 R5.

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.5
	ADV_IMP.1
	ADV_INT.2
	ADV_TDS.4
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.4
	ALC_CMS.5
	ALC_DEL.1
	ALC_DVS.2
	ALC_LCD.1
	ALC_TAT.2
ATE	ATE_COV.2
	ATE_DPT.3
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.5

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
FPT_PHP.3
FDP_ITT.1
FDP_IFC.1
FPT_ITT.1
FDP_SDC.1
FDP_SDI.2
FCS_RNG.1[PTG.2]
FCS_COP.1[TDES]
FCS_COP.1[RSA-CRT]

IDENTIFICATION

Product: THN31 Secure Element version 1.0.

Security Target: THN31 Secure Element version 1.0 Security Target, version 2.0 (May 2023).

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 EAL5 + ALC_DVS.2 + AVA_VAN.5.

SECURITY POLICIES

The use of the product THN31 Secure Element 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 THN31 Secure Element version 1.0, although the agents implementing attacks have the attack potential according to the High of EAL5 + ALC_DVS.2 + AVA_VAN.5 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. Boot mode is the initial mode after the chip is powered up. This mode is not available to the Security IC embedded software. It can either switch to test mode under the purpose of testing or initialization, or switch to normal mode.

2. 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.

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

The TOE provides ROM for executing the boot code and Crypto Library code, NVM for Crypto SU library code, the other 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 SPI interface, ISO/IEC 7816 contact interface, SWP interface and I2C interface.

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, bus masking and random OSC clock jitter which configures 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 checks 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.

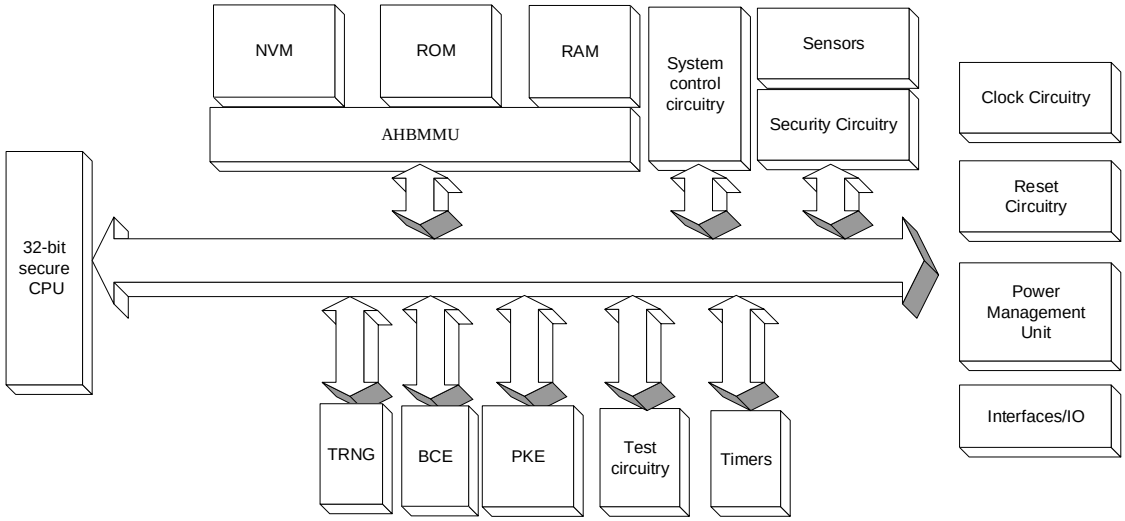
The TOE provides a true random number generator, which is accessible by the crypto library. The true random number generator is composed of entropy sources, self-test circuit and post-processing circuit. The self-test circuit includes the total failure test and online test. The total failure test is 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

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
  - SWP interface
  - ISO/IEC 7816 contact interface
  - SPI interface
  - I2C interface

- True Random Number Generator
- Block Cryptography Engine for TDES supporting
- Public-Key Engine for RSA-CRT supporting
- System control circuitry
- Test circuitry
- Timers
- Security Circuitry
- Sensors
    - Voltage sensor
    - Glitch sensor
    - Frequency sensor
    - Temperature sensor
    - Light sensor
- Power Management Circuitry
- Clock circuitry
- 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.

- THN31 Secure Element version 1.0 Security Target Lite, version 1.0
- THN31 Secure Element version 1.0 Preparative Guidance, Version 1.3
- THN31 Secure Element version 1.0 Operational Guidance, Version 1.4
- THN31 Secure Element version 1.0 Security Guidelines, Version 1.8
- THN31 Secure Element version 1.0 Cryptographic Algorithm API, Version 1.6

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 has repeated all the developer functional tests in the evaluator premises.

In addition, the lab has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer. 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 85.71% of the SFRs and 58.33% of the TSFIs defined in the Functional Specification has 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 [JILAAPS] and [JILADVARC]. 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 High 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 software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product THN31 Secure Element version 1.0 it is necessary the disposition of the following components:

- THN31 HW module.
- Crypto Library.
- Crypto SU 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	THN31	1.0	Module
Software	Crypto Library	2.1.0	Software library in ROM
	Crypto SU library	2.11	Software library in NVM
	Boot code	1.0	Boot in ROM
	Header file	0.1	cryptolib.h

EVALUATION RESULTS

The product THN31 Secure Element version 1.0 has been evaluated against the Security Target THN31 Secure Element version 1.0 Security Target, version 2.0 (May 2023).

All the assurance components required by the evaluation level EAL5 + ALC_DVS.2 + AVA_VAN.5 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 EAL5 + ALC_DVS.2 + AVA_VAN.5, 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 THN31 Secure Element version 1.0, a positive resolution is proposed.

The 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 THN31 Secure Element version 1.0 Security Guidelines, 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 THN31 Secure Element version 1.0 Security Guidelines, version 1.8; otherwise, the certificate is not applicable.

The TOE consumer should also observe the application notes defined in the applicable security target. The recommended cryptographic algorithms and key lengths are those defined in SOGIS Agreed Cryptographic Mechanisms, version 1.2. All other algorithms and key lengths are out of the scope of the certificate. The algorithms and key sizes within the scope of the certificate are described in the table below.

CRYPTOGRAPHIC MECHANISM	STANDARD OF IMPLEMENTATION	KEY/MODULE SIZE [BITS]	AGREED CRYPTOGRAPHIC MECHANISMS v1.2
TDES-ECB (Encryption, decryption)	NIST SP800-67 Rev.2 NIST SP800-38A 2001 ED	112 168	NOT INCLUDED
RSA-CRT (decryption)	PKCS #1 v2.2	1900-2999	LEGACY
		3000 - 4096	RECOMMENDED

The Certification Body considers necessary to remark that PDMC uses MD5 algorithm for integrity verification of the logical mask data sent by UMC. This algorithm is not included in SOGIS Agreed Cryptographic Mechanisms (version 1.2), not even as legacy. This fact was communicated to the laboratory which answer was that "*the use of MD5 is the formal procedure defined in the scope of the delivery procedures of the UMC sites, which are covered by the certificates of the UMC sites under the BSI scheme (BSI-DSZCC-S 0228 and BSI-DSZ-CC-S-0201-2022). Therefore, the results of this certified procedure of the UMC sites are being reused and the evaluator considers this MD5 integrity validation procedure as acceptable, for consistency with the BSI certificates of the UMC sites*".

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.

[JILAAPS] Application of Attack Potential to Smartcards, version 2.9. Jan.2013. Joint Interpretation Library.

[JILADVARC] Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices, version 2.2. Jan. 2013. Joint Interpretation Library.

[CCDB-2006-04-004] Common Criteria. Additional CCRA Supporting Documents. ST sanitising for publication. Document number 2006-04-004, April 2006.

[ST] THN31 Secure Element version 1.0 Security Target, version 2.0 (May 2023).

[ST Lite] THN31 Secure Element version 1.0 Security Target Lite, version 1.0 (Sep 2023).

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:

- THN31 Secure Element version 1.0 Security Target, version 2.0 (May 2023).

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:

- THN31 Secure Element version 1.0 Security Target Lite, version 1.0 (Sep 2023).

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. THN31 Secure Element version 1.0.
- **Report ID**: CCETMS001.
- **Version**: M1.
- **Issue Date**: 18/01/2024.
- **SHA256**: 8ca1f17b4426a66ca095d8fc123264fde1905c3da001f0786979d56048dd770c
- **Issuing ITSEF**: Applus Laboratories.

- **Validity expiration date**: 06/07/2025.

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 (including the STAR report) with third parties.

It is expected that if the applicant Beijing TsingTeng MicroSystem 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 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 EAL1 to EAL4 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 EAL2 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 EAL4 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.