Certification Report

TMCOS 4.0 0.3 on THD89 1.0.3 Secure Element Java Card System Platform, version v4.0 0.3

Sponsor:	***Tongxin Microelectronics Co., Ltd.*** **401, F/4, B-1 Building, Zhongguancun Dongsheng Technology Park Northern Territory, No.66 XiXiaokou Road** **Haidian District** **Beijing** **China**
Developer:	***Beijing Tsingteng Microsystem Co., Ltd.*** **401, F/4, B-1 Building, Zhongguancun Dongsheng Technology Park Northern Territory, No.66 XiXiaokou Road** **Haidian District** **Beijing** **China**
Evaluation facility:	***Keysight Technologies Netherlands Riscure B.V.*** **Delftechpark 49** **2628 XJ Delft** **The Netherlands**
Report number:	**NSCIB-CC-2400175-01-CR**
Report version:	**1**
Project number:	NSCIB-**2400175-01**
Author(s):	**Jordi Mujal**
Date:	**24 January 2025**
Number of pages:	**11**
Number of appendices:	**0**

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the TMCOS 4.0 0.3 on THD89 1.0.3 Secure Element Java Card System Platform, version v4.0 0.3. The developer of the TMCOS 4.0 0.3 on THD89 1.0.3 Secure Element Java Card System Platform, version v4.0 0.3 is Beijing Tsingteng Microsystem Co., Ltd. located in Beijing, China and Tongxin Microelectronics Co., Ltd. was the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE type is an Embedded Secure Element that implements Java Card System and is deployed on a certified IC hardware. This TOE affords the security services including loading, installation and instantiation of applets before and after issuance, and secure execution of Java Card applets that are verified off-card.

The TOE has been evaluated by Keysight Technologies Netherlands Riscure B.V. located in Delft, The Netherlands. The evaluation was completed on 24 January 2025 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*. The TOE is exactly the same as the one certified under NSCIB-2400034-01 but the current certification is the result of just changing the sponsor name.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the TMCOS 4.0 0.3 on THD89 1.0.3 Secure Element Java Card System Platform, version v4.0 0.3, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the TMCOS 4.0 0.3 on THD89 1.0.3 Secure Element Java Card System Platform, version v4.0 0.3 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the TMCOS 4.0 0.3 on THD89 1.0.3 Secure Element Java Card System Platform, version v4.0 0.3 from Beijing Tsingteng Microsystem Co., Ltd. located in Beijing, China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	THD89 1.0.3 Secure Element	1.0.3
Firmware	Crypto Library	2.1.0
	Crypto SU Library	2.2.0
	CryptoECCSec Library	1.0.0
Software	TMCOS	4.0 0.3

To ensure secure usage a set of guidance documents is provided, together with the TMCOS 4.0 0.3 on THD89 1.0.3 Secure Element Java Card System Platform, version v4.0 0.3. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST-Lite]*, Chapter 1.5.3.

2.2 Security Policy

The TOE includes the following cryptographic features:

- EC Key generation
- 3DES encryption, decryption, and MAC
- RSA-CRT signature generation
- ECDSA signature generation and verification
- AES CBC/ECB Encryption and Decryption, MAC, CMAC

The TOE provides the following Java Card v3.1 features:

- Executing Java Card bytecodes.
- Managing memory allocation of code and data of applets.
- Managing linkage of CAP file resources and contained applets.
- Enforcing access rules between applets and the JCRE.
- Mapping of Java method calls to native implementations e.g. cryptographic operation.
- Garbage Collection fully implemented with complete memory reclamation including compactification.
- Persistent Memory Management and Transaction Mechanism.
- Array views on array objects.

The TOE provides the following GlobalPlatform Card Specification v2.3 features:

- Package loading and installation
- Package extradition
- Security domain personalization
- Applet uninstallation

• Package deletion

• Privilege managements

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

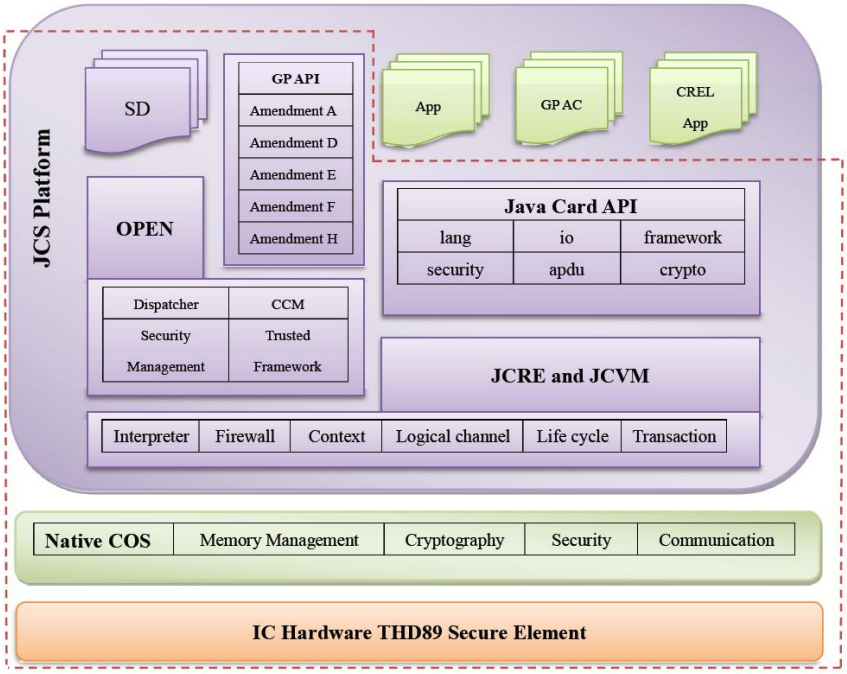
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 1.5.3 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The TOE architecture as it is presented in the [ST] is depicted as:



2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
TMCOS 4.0 0.3 On THD89 1.0.3 Preparative procedures	1.4
TMCOS 4.0 0.3 On THD89 1.0.3 Operational User Guidance	1.6

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer performed extensive testing on functional specification, subsystem and SFR-enforcing module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

The underlying hardware and crypto-library test results are extendable to composite evaluations, because the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent penetration testing

The vulnerability analysis was performed considering each SFR, based on the structure of the attack methods defined by *[JIL-AAPS]* and *[JIL-AMS]*.

The total penetration testing effort expended by the evaluators was 7 weeks. During the test campaign out of the total effort spent on penetration testing; 0% was on physical attacks, 0% was on overcoming sensors and filters, 29% was on perturbation attacks, 0% was on retrieving keys with FA, 42% was on side-channel attacks, 0% was on exploitation of test features, 0% was on attacks on RNG, 0% was on ill-formed Java Card applications, 29% was on software attacks, and 0% was on application isolation penetration tests.

2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the *[ST]*.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential". The TOE supports a wider range of key sizes (see *[ST]*), including those with sufficient algorithmic security level to exceed 100 bits as required for high attack potential (AVA_VAN.5).

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities.

For composite evaluations, please consult the *[ETRfC]* for details.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of three Site Technical Audit Reports.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number TMCOS 4.0 0.3 on THD89 1.0.3 Secure Element Java Card System Platform, version v4.0 0.3.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents. To support composite evaluations according to *[COMP]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that must be considered when this TOE is used as platform in a composite evaluation.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the TMCOS 4.0 0.3 on THD89 1.0.3 Secure Element Java Card System Platform, version v4.0 0.3, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with ALC_DVS.2 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'demonstrable' conformance to the Protection Profile *[PP]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: none.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength to satisfy the AVA_VAN.5 "high attack potential". To be protected against attackers with a "high attack potential", appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

3 Security Target

The TMCOS 4.0 0.3 on THD89 1.0.3 Secure Element Java Card System Platform Security Target, Tongxin Microelectronics Co., Ltd., version 0.3, 24 January 2025 *[ST]* is included here by reference.

Please note that, to satisfy the need for publication, a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
DES	Data Encryption Standard
DFA	Differential Fault Analysis
ECB	Electronic Code Book (a block-cipher mode of operation)
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EMA	Electromagnetic Analysis
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MAC	Message Authentication Code
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SPA/DPA	Simple/Differential Power Analysis
TOE	Target of Evaluation
TRNG	True Random Number Generator

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018
[ETR]	Evaluation Technical Report for TMCOS on THD89 1.0.3 SE Java Card System Platform V4.0 0.3, 20230529-D13, NSCIB-2400175-01, version 1.1, 24 January 2025
[ETRfC]	ETR for composite evaluation TMCOS on THD89 1.0.3 SE Java Card System Platform V4.0 0.3, 20230529-D14, NSCIB-2400175-01, version 1.1, 24 January 2025
[HW-CERT]	CERTIFICATION REPORT CCN-CC/2021-36/INF-4157, 2021-36-INF-4157-v1, 25 September 2023
[HW-ETRfC]	ETR for composite evaluation, CCETMC003-ETRfC-M1, 15 May 2024
[HW-ST-Lite]	THD89 1.0.3 Secure Element Version 1.0 Security Target Lite, version 0.1 Jun. 2023
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.2.1, February 2024
[JIL-AMS]	Attack Methods for Smartcards and Similar Devices, Version 2.5, May 2022 (sensitive with controlled distribution)
[PP0099]	Java Card System - Open Configuration Protection Profile, version 3.1, April 2020, registered under the reference BSI-CC-PP-0099-V2-2020
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	TMCOS 4.0 0.3 on THD89 1.0.3 Secure Element Java Card System Platform Security Target, Tongxin Microelectronics Co., Ltd., version 0.3, 24 January 2025
[ST-lite]	TMCOS 4.0 0.3 on THD89 1.0.3 Secure Element Java Card System Platform Security Target Lite, Tongxin Microelectronics Co., Ltd., version 1.2, 24 January 2025
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)