Certification Report

FM1280 07 Dual Interface Smart Card Chip with IC Dedicated Software 2.77

Sponsor and developer: ***Shanghai Fudan Microelectronics Group Company Limited***
Building 4, No.127, GuoTai Road
Shanghai
P.R. China

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-2300106-01-CR**

Report version: **1**

Project number: NSCIB-**2300106-01**

Author(s): **Kjartan Jæger Kvassnes**

Date: **01 October 2025**

Number of pages: **12**

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.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

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 FM1280 07 Dual Interface Smart Card Chip with IC Dedicated Software 2.77. The developer of the FM1280 07 Dual Interface Smart Card Chip with IC Dedicated Software 2.77 is Shanghai Fudan Microelectronics Group Company Limited located in Shanghai, P.R.C. and they also act as 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 is a FM1280 07 Dual Interface Smart Card Chip with IC Dedicated Software 2.77, in short FM1280, developed by Shanghai Fudan Microelectronics. It can be widely and easily applied in various security fields.

The FM1280 consists of the IC Hardware, the IC Dedicated Software and the supporting documents.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 01 October 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 scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the FM1280 07 Dual Interface Smart Card Chip with IC Dedicated Software 2.77, 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 FM1280 07 Dual Interface Smart Card Chip with IC Dedicated Software 2.77 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 FM1280 07 Dual Interface Smart Card Chip with IC Dedicated Software 2.77 from Shanghai Fudan Microelectronics Group Company Limited located in Shanghai, P.R.C..

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	FM1280 07	07
Software	IC Dedicated Firmware which includes the following:	2.77
	FMSH_CryptoLib	3.110
	FM_CryptoLib.h FM_CryptoLib_struct.h FM_Firmware_staticLib_Crypto.lib	2.01
	Driver	1.00
	FM_DriverAPI.h FM_Firmware_staticLib_Driver.lib	1.12
	AU library	06

To ensure secure usage a set of guidance documents is provided, together with the FM1280 07 Dual Interface Smart Card Chip with IC Dedicated Software 2.77. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]* or *[ST-Lite]*, Chapter 1.4.

2.2 Security Policy

The TOE has the following security features:

- Hardware coprocessor for TDES
- Hardware coprocessor for AES
- True Random Number Generator with protections
- Hardware for RSA support
- Protection against power and electronic magnetic analysis
- Protection against physical attacks
- Protection against perturbation attacks
- Memory access control
- Memory encryption
- Data and critical register protection
- Active shielding
- Security sensors
- Software library with cryptographic services

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

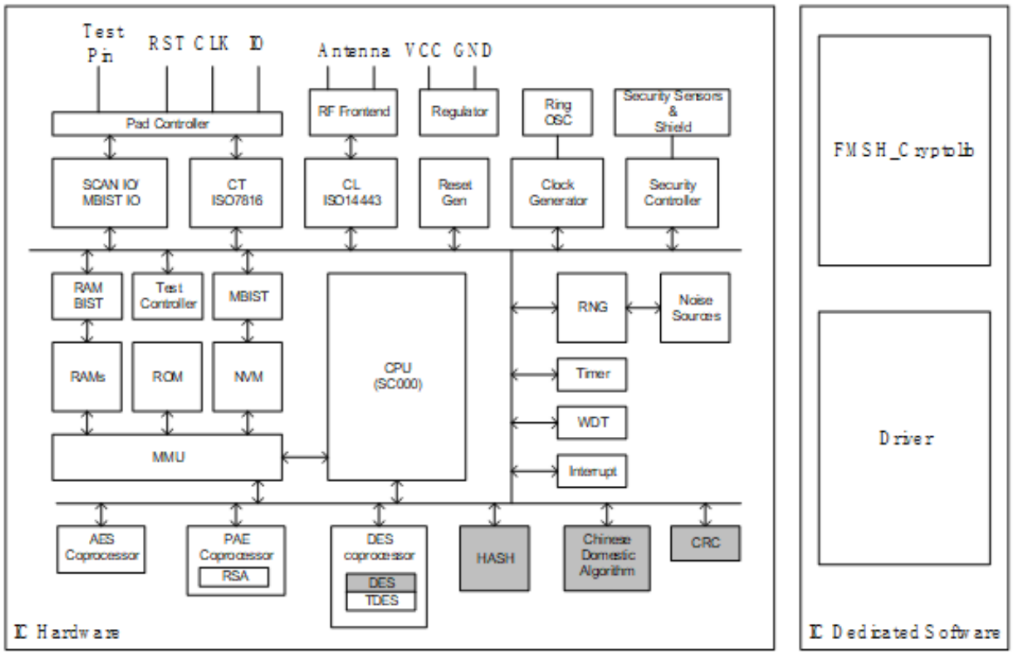
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 and 4.3 of the *[ST]* or *[ST-Lite]*.

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 logical architecture of the TOE can be depicted as follows:



2.5 Documentation

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

Identifier	Version
FM1280 07 Security Preparatory Guidance, Dated March 2025	V0.7
FM1280 07 Security Programming Guidance, Dated March 2025	V0.7
FM1280 07 Application Programming Interface for FMSH_CryptoLib, Dated October 2023	V0.3
FM1280 07 Application Programming Interface for Driver, Dated August 2023	V0.2
FM1280 07 User Manual, Dated February 2024	V1.3

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.

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 methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review is performed on the TOE. During this attack-oriented analysis, the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this analysis will be performed according to the attack methods in [JIL-AM].
- All potential vulnerabilities are analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.
- Due to the long evaluation time period, the source code was reviewed again and re-testing was performed in 2025 to validate the previous test results.

The total test effort expended by the evaluators was 50 weeks. During that test campaign, 5% of the total time was spent on physical attacks, 26% on Perturbation attacks, 47% on side-channel testing, and 5% on logical tests.

2.6.3 Test configuration

The testing was performed on the following configuration:

- Hardware: FM1280 07
- IC Dedicated Software: 2.77
    - CryptoLib: 3.110
    - Crypto.lib: 2.01
    - Driver: 1.000
    - Driver.lib: 1.12
    - AU library: 05/06

      Note that the updated RSA function in AU library is tested against AU library version v06. Other parts of the TOE components were tested against AU library v05. The evaluator confirmed the results for version 05 are also valid for 06.

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.

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

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 4 site audit reports, 1 site certificate and 1 Site Technical Audit Report.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number FM1280 07 Dual Interface Smart Card Chip with IC Dedicated Software 2.77.

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 FM1280 07 Dual Interface Smart Card Chip with IC Dedicated Software 2.77, 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 'strict' conformance to the Protection Profile *[PP_0084]*.

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.

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 FM1280 07 Dual Interface Smart Card Chip with IC Dedicated Software Security Target, v0.9, 22 June 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:

IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
RNG	Random Number Generator
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 “FM1280 07 Dual Interface Smart Card Chip with IC Dedicated Software” – EAL5+, 23-RPT-1471, Version 8.1, Dated 13 August 2025
[ETRfC]	Evaluation Technical Report for Composition “FM1280 07 Dual Interface Smart Card Chip with IC Dedicated Software 2.77” – EAL5+, 24-RPT-958, Version 6.1, Dated 13 August 2025
[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)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[PP_0084]	Security IC Platform Protection Profile with Augmentation Packages, registered under the reference BSI-CC-PP-0084-2014, Version 1.0, 13 January 2014
[ST]	FM1280 07 Dual Interface Smart Card Chip with IC Dedicated Software Security Target, v0.9, 22 June 2025
[ST-lite]	FM1280 07 Dual Interface Smart Card Chip with IC Dedicated Software 2.77 Security Target Lite, v1.2, dated March 2025
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)