Certification Report

MF3D(H)x3

Sponsor and developer:	***NXP Semiconductors Germany GmbH*** **Business Unit Security & Connectivity, Troplowitzstrasse 20, D-22529 Hamburg, Germany**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-0011955-CR2**
Report version:	**1**
Project number:	**0011955_2**
Author(s):	**Andy Brown**
Date:	**10 March 2023**
Number of pages:	**11**
Number of appendices:	**0**

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

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, TÜV Rheinland Nederland 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 TÜV Rheinland Nederland 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 TÜV Rheinland Nederland 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, TÜV Rheinland Nederland 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

The 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. Check whether this section is appropriate; if not, remove the relevant logo and section(s).

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 MF3D(H)x3. The developer of the MF3D(H)x3 is NXP Semiconductors Germany GmbH located in Hamburg, Germany 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 to be used with Proximity Coupling Devices (PCDs, also called "terminal") according to ISO 14443 Type A. It is primarily designed for secure contactless transport applications and related loyalty programs as well as access control management systems as well as closed loop payment systems.

The TOE is a smart card comprising a hardware platform and a fixed software package. The software package is stored in Flash and ROM memory and provides an operating system with a set of functions, used to manage the various kinds of data files stored in Flash memory. The operating system supports a separation between the data of different applications and provides access control if required by the configuration.

The TOE includes also IC Dedicated Software to support its start-up and for test purposes after production. The Smart Card Controller hardware comprises a 16-bit CPU, volatile and non-volatile memories, cryptographic co-processors, security components and one communication interface.

The TOE was evaluated initially by SGS Brightsight B.V. located in Delft, The Netherlands and was certified on 16/04/2020. The re-evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 10 March 2023 with the approval of the *[ETR]*. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

This second issue of the Certification Report is a result of a “recertification with major changes”.

The major changes are:

An additional production facility has been added to the lifecycle of the TOE.

An updated ROM code to incorporate previous patches in the main code and to support the 16kB versions of MF3D(H)x3.

The security evaluation reused the evaluation results of previously performed evaluations. A full, up-to-date vulnerability analysis has been made, as well as renewed testing.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the MF3D(H)x3, 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 MF3D(H)x3 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).

TÜV Rheinland Nederland 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 MF3D(H)x3 from NXP Semiconductors Germany GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
IC Hardware	MF3D(H)x3 Hardware	A1.A04 A1.A05
IC Dedicated Test Software	Test Software	A1.A04 A1.A05
IC Dedicated Support Software	Boot Software	A1.A04 A1.A05
	Firmware	A1.A04 A1.A05
	MIFARE DESFire Software	3.0

To ensure secure usage a set of guidance documents is provided, together with the MF3D(H)x3. For details, see section 0 “The **IC Hardware** CPU has a 16-bit architecture. The on-chip hardware components are controlled by the MIFARE DESFire software via Special Function Registers. These registers are correlated to the activities of the CPU, the memory management unit, interrupt control, contactless communication, Flash, timers, the DES co-processor and the AES co-processor. The communication with the MF3D(H)x3 can be performed through the contactless interface.

The **IC Dedicated Test Software** (Test ROM Software) located in ROM of the TOE is used by the TOE Manufacturer to test the functionality of the chip. The test functionality is disabled before the operational use of the smart card. The IC Dedicated Test Software includes the test operating system, test routines for the various blocks of the circuitry and shutdown functions to ensure that security relevant test operations cannot be executed illegally after phase 3 of the TOE Life cycle.

The **IC Dedicated Support Software** contains Boot Software, Firmware and MIFARE DESFire Software. The **Boot Software** ensures that the TOE is booting after reset in a correct manner. The **Firmware** component provides memory management functionality and cryptographic library that performs the cryptographic operations required for this TOE. Finally, the **MIFARE DESFire Software** contains the relevant functionality required for the MIFARE features including a flexible file system, authentication, data encryption and other features. The features of the TOE are described in detail in Section 1.4.2 [ST].
Documentation” of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 1.4.3.

2.2 Security Policy

The TOE is a smart card comprising a hardware platform and a fixed software package. The TOE is to be used with Proximity Coupling Devices (PCDs, also called "terminal") according to ISO 14443 Type A. The communication protocol complies to part ISO 14443-4.

Cryptographic functionality provided by the TOE includes Triple-DES (3DES) and AES, including CMAC and various modes of operation (e.g. CBC). Furthermore, the TOE provides hardware random number generation according to class PTG.2 of AIS 31.

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 4.3 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.

For DESFire EV1 backward compatible mode, the certification scope is limited to the AES mode (both for authentication and secure messaging) and 3TDEA (only authentication). Please note that the MIFARE DESFire D40 backward compatible mode is not part of any SFR and therefore not in the certification scope. Also the MIFARE Classic compatible mode, including all DESFire applications that enable MIFARE Classic mapping, are excluded from the certification scope

2.4 Architectural Information

The **IC Hardware** CPU has a 16-bit architecture. The on-chip hardware components are controlled by the MIFARE DESFire software via Special Function Registers. These registers are correlated to the activities of the CPU, the memory management unit, interrupt control, contactless communication, Flash, timers, the DES co-processor and the AES co-processor. The communication with the MF3D(H)x3 can be performed through the contactless interface.

The **IC Dedicated Test Software** (Test ROM Software) located in ROM of the TOE is used by the TOE Manufacturer to test the functionality of the chip. The test functionality is disabled before the operational use of the smart card. The IC Dedicated Test Software includes the test operating system, test routines for the various blocks of the circuitry and shutdown functions to ensure that security relevant test operations cannot be executed illegally after phase 3 of the TOE Life cycle.

The **IC Dedicated Support Software** contains Boot Software, Firmware and MIFARE DESFire Software. The **Boot Software** ensures that the TOE is booting after reset in a correct manner. The **Firmware** component provides memory management functionality and cryptographic library that performs the cryptographic operations required for this TOE. Finally, the **MIFARE DESFire Software** contains the relevant functionality required for the MIFARE features including a flexible file system, authentication, data encryption and other features. The features of the TOE are described in detail in Section 1.4.2 [ST].

2.5 Documentation

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

Identifier	Version
MF3D(H)x3, MIFARE DESFire EV3 contactless smartcard IC, Product data sheet	3.3
MF3D(H)x3C, MIFARE DESFire EV3C contactless smartcard IC, Product data sheet (for MFC unlocked configurations only)	3.5
MF3D(H)x3, MIFARE DESFire EV3 Post Delivery Configuration, Preliminary data sheet addendum	2.0
MF3D(H)x3, Wafer and Delivery Specification, Product data sheet addendum	3.3

MF3D(H)x3, Information on Guidance and Operation, Guidance and Operation Manual	1.3

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 has performed extensive testing on FSP, subsystem and SFR-enforcing module and module interface level. The tests are performed by the developer through execution of test scripts using an automated and distributed system. Test tools and scripts are extensively used to verify that the tests return expected values. The identification was checked based on the SVN revision corresponding to the version control system repository.

The tests covered all security functions and aspects of the TSF. To further support the hardware, component testing was used that verifies several aspects e.g. return values, registers, CPU and others in an automated manner. Code coverage analysis was used by the developer to verify overall test completeness.

For the testing performed by the evaluators, repeated/witnessed tests have been selected that cover various aspects of the TOE, as well as test areas of the developer code coverage analysis. Additionally, witness testing was used to sample and check the actual test results.

The evaluator-defined tests were focussed on supplementing the developer's tests since the developer tests are extensive. Three evaluator defined tests were performed.

For the testing performed by the evaluators, the developer has provided samples and a test environment.

2.6.2 Independent penetration testing

The penetration tests were devised after performing the evaluator Vulnerability Analysis. Potential vulnerabilities were identified via review of evidence for the classes ADV, AGD, ASE and ADV_IMP. For ADV_IMP a thorough implementation representation review was performed on the TOE. Potential vulnerabilities were grouped per similarity and addressed by penetration testing aiming at the weakest case.

Vulnerability Analysis activities were performed for each group of components with the vulnerability analysis for the MIFARE DESFire Software also considering the TOE in its entirety.

In the baseline certification 30% of the test effort expended by the evaluators was on perturbation attacks, 50% on side channel attacks and 20% on software attacks.

For this first re-certification 100% of the test effort expended by the evaluators was spent on perturbation attacks.

2.6.3 Test configuration

The developer provided the environment for independent evaluation testing. The TOE was tested in all memory sizes in the following configurations:

- FPGA Emulator
- TOE (SO28 package)
- Using ISO14443 interface

For penetration testing, the TOE was tested in configurations commensurate to MF3Dx3 (with 8KB storage size) as present in the version control system repository corresponding to MIFARE DESFire 3.0 with hardware A1.A04.

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.

The algorithmic security level exceeds 100 bits for all evaluated cryptographic functionality as required for high attack potential (AVA_VAN.5).

2.7 Reused Evaluation Results

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been reused, but vulnerability analysis and penetration testing has been renewed.

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 18 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 MF3D(H)x3.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*.

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

Based on the above evaluation results the evaluation lab concluded the MF3D(H)x3, 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]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 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 with respect to the resistance against certain attacks.

For clarity on the scope of backward compatibility and certification see section 2.3.2.

In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to 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. In order for the evolution of attack methods and techniques to be covered, he 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***

3 Security Target

The MF3D(H)x3 Security Target, Rev. 2.4, 04 January 2023 *[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:

CBC	Cipher Block Chaining (a block cipher mode of operation)
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

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
[ETR]	Evaluation Technical Report MF3D(H)x3, 20-RPT-082, Version 1.0, 09 April 2020 amended by Evaluator Assessment of Changes Report (EAR) NXP MF3D(H)x3, 22-RPT-1219, Version 4.0, 08 March 2023
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[PP]	Security IC Platform Protection Profile with Augmentation Packages, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014, Version 1.0, 13 January 2014
[ST]	MF3D(H)x3 Security Target, Rev. 2.4, 04 January 2023
[ST-lite]	MF3D(H)x3 Security Target Lite, Rev 2.4, 04 January 2023
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)