Certification Report

MF3Dx2 v2

Sponsor and developer:	***NXP Semiconductors Germany GmbH*** **Troplowitzstrasse 20, 22529 Hamburg** **Germany**
Evaluation facility:	***Brightsight*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-207017-CR**
Report version:	**1**
Project number:	**207017**
Author(s):	**Denise Cater**
Date:	**29 January 2019**
Number of pages:	**13**
Number of appendices:	**0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Headoffice:
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 Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

Certificate

Standard
Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)

Certificate number
CC-19-207017

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer
NXP Semiconductors Germany GmbH

Troplowitzstrasse 20, 22529 Hamburg, Germany

Product and assurance level
MF3Dx2 v2

Assurance Package:

- EAL5 augmented with AVA_VAN.5 and ALC_DVS.2

Protection Profile Conformance:

- Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, registered and certified by Bundesamt fuer Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0084-2014 dated 13 January 2014

Project number
207017

Evaluation facility
Brightsight BV located in Delft, the Netherlands

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL7

Validity
Date of 1st issue : **01-02-2019**
Certificate expiry : **01-02-2024**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

C.C.M. van Houten, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

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 license 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, in order 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 authorized provided the report is reproduced in its entirety.

Recognition of the certificate

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

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 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. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the MF3Dx2 v2. The developer of the MF3Dx2 v2 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 a Secure Smart Card Controller [ST] to be used with Proximity Coupling Devices (PDCs, also called “terminal”) according to ISO/IEC 14443 Type A [ISO14443].

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 has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 28 January 2019 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 MF3Dx2 v2, 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 MF3Dx2 v2 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]*.

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. It should be noted that the certification results only apply 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 releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the MF3Dx2 v2 from NXP Semiconductors Germany GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Component type	Name	Version	Form of delivery
IC Hardware	MF3Dx2 v2 Hardware	22.0	Wafer (FFC), Modules (MOB4, MOB6)
IC Dedicated Test Software	Test Software	9.2.3	On-chip Software
IC Dedicated Support Software	Boot Software	9.2.3	On-chip Software
	Firmware	9.2.3	On-chip Software
	MIFARE DESFire Software	2.2	On-chip Software

To ensure secure usage a set of guidance documents is provided together with the MF3Dx2 v2. Details can be found in section ”Documentation” of this report.

The configurations as listed in [ST] Section 1.4.1.1, are indicated according to the format MF3D(H)x2 with the following meaning:

Identifier	Description	Assignment	Meaning
x	Memory size	2 4 8 9 A	2KB of memory available. 4KB of memory available. 8KB of memory available. 16KB of memory available. 32KB of memory available.
(H)	Input capacitance	Present Absent	70pF 17pF

The customer can check the version of the IC Hardware and IC Dedicated Software by using the verification method described in Section 3.1 of the Guidance and Operation Manual (see section ”Documentation” of this report).

For a detailed 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, which can be used with Proximity Coupling Devices (also called "terminal") according to ISO 14443 Type A. The communication protocol complies to part ISO 14443-4.

Cryptographic functionality provide by the TOE includes Triple-DES (3DES) and AES, including CMAC and various modes of operation (e.g. ECB, 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

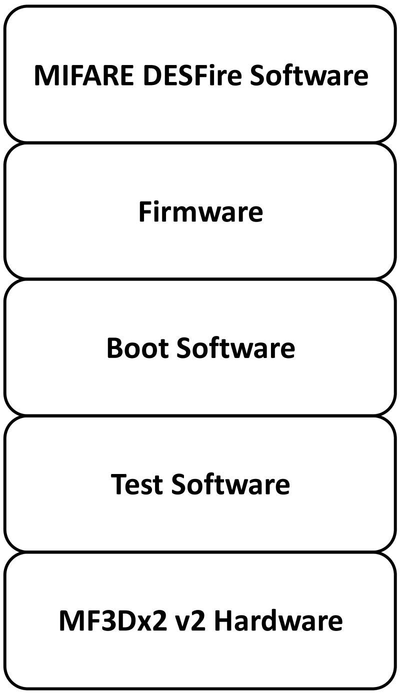
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 4.3 of the *[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.

2.4 Architectural Information

The components of the TOE can be depicted as follows:



The **Hardware** component provides the CPU, memory management, interrupt control, contactless communication, Flash memory and the DES and AES co-processors and hardware Random Number Generator. The **Test Software** component includes test functionality for the various blocks of the circuitry and shutdown functions to ensure that security relevant test operations cannot be executed illegally after phase three of the TOE life cycle. 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
MF3Dx2 v2, Information on Guidance and Operation, Guidance and Operation Manual	Rev. 1.3 dated 16 January 2019

MF3Dx200Dpp(p)/02, MIFARE DESFire EV2 contactless smartcard IC, Objective data sheet[2]	Rev. 1.1 dated 17 January 2019
MF3D92/MF3DA2, MIFARE DESFire EV2 16KB and 32KB contactless smartcard IC, Objective data sheet[3]	Rev. 1.1 dated 17 January 2019

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 functional specification, subsystem and SFR-enforcing module level.

The following test configurations were used, divided based on the components, i.e.:

- Hardware, Boot Software and Test Software
    - Tests for Flash are executed for either maximum size or in the case of simulation tests, with random memory configurations.
    - Tests cover all variations of modes that the hardware and software offers
    - Test and TOE code are taken directly from the developer CMS
    - A total of eleven tests were repeated/witnessed by the evaluator
- Firmware
    - Firmware and Cryptographic Library located in ROM
    - Primary test mode is for Cryptographic Library in Flash as it is a weaker target and more possibilities exist to test internal functions, i.e. better coverage
    - Configurations where subset of Cryptographic Library is in ROM are also tested
    - A total of ten tests were repeated/witnessed by the evaluator
- MIFARE DESFire Software
    - The variation on this component is the configuration of available memory size.
    - Black-box tests are required to pass for all sizes.
    - A total of nine tests were witnessed by the evaluator.

The evaluator-defined tests were supported by a Brightsight-developed Test OS. The evaluator defined tests with a division based on the components. For the **Hardware**, **Boot Software** and **Test Software**, a total of nine tests were performed. Focus was put on sensors and active shield, firewall, RNG, PUF and AES encryption. For the **Firmware**, a total of twelve tests were performed. Focus was put on cryptographic functions, key integrity and handling and memory operations. For the **MIFARE DESFire Software**, a total of two tests were performed. Focus was put on search for hidden interfaces and commands and abnormal execution sequences (fuzzing) targeting robustness of command and state handling. The tests for **MIFARE DESFire Software** exercised all the components listed.

2.6.2 Independent Penetration Testing

The penetration tests are devised after performing the Evaluator Vulnerability Analysis.

Vulnerability analysis activities were performed for each group of components, as described below, with the vulnerability analysis for the MIFARE DESFire Software also considering the TOE in its entirety:

- Hardware, Boot Software and Test Software.
    - A total of ten perturbation penetration tests were performed targeting various hardware building blocks including the CPU, registers, memory, RNG, co-processors and the boot flow. A total of six side channel analysis penetration tests were performed targeting various cryptographic operations and key management functions and a

[2] Only for 2KB, 4KB and 8KB.

[3] Only for 16KB and 32 KB.

further four characterization tests for sensors and other critical functions. Finally, a total of two physical penetration tests were performed targeting sensors and bus interface.

- Firmware
  - A total of thirteen side channel analysis penetration tests (including template attacks and deep learning) were performed along with six perturbation penetration tests specifically targeting cryptographic and key operations.
- MIFARE DESFire Software
  - The tests for DESFire Software exercise the TOE (i.e. all the components listed) and included a total two perturbation attacks targeting authentication and file operations.

2.6.3 Test Configuration

The test configurations are described in "*Testing approach and depth*" section above. The evaluator tests were performed using samples of the 32KB memory size product.

2.6.4 Testing 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 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). Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential".

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities. These activities revealed that for some cryptographic functionality the security level could be reduced from an algorithmic security level above 100 bits to a practical remaining security level lower than 100 bits. As the remaining security level still exceeds 80 bits, this is considered sufficient. So no exploitable vulnerabilities were found with the independent penetration tests.

2.7 Re-used evaluation results

There has been extensive re-use of the ALC aspects for the sites involved in the development and production of the TOE. A total of nine Site Technical Audit Reports (STARs) were available, three Site Re-use Reports, seven ETR-Lite reports and two Shared Audit Reports (SARs) from other evaluations were used.

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 MF3Dx2 v2, as described in the identification part of this report.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[4] which references a ASE Intermediate Report and other evaluator documents.

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

The verdict of each claimed assurance requirement is “**Pass**”.

Based on the above evaluation results the evaluation lab concluded the MF3Dx2 v2, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with AVA_VAN.5** and ALC_DVS.2. 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.

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.

An *Originality Check* procedure can be performed as described in Section 3.2 of the Guidance and Operation Manual (see section “Documentation” of this report) to detect counterfeit products.

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.

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

3 Security Target

The MF3Dx2 v2, Security Target, Rev. 1.2 dated 17 January 2019 *[ST]* is included here by reference.

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

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

AES	Advanced Encryption Standard
CMS	Configuration Management Systems
DES	Data Encryption Standard
EMA	Electromagnetic Analysis
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 MF3Dx2 v2 , 19-RPT-047, version 2.0, dated 28 January 2019.

[ISO14443] ISO/IEC 14443-3, First Edition, Amendment 1, 1 June 2005 and ISO/IEC 14443-4, Second Edition, 15 July 2008.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.4, 27 September 2017.

[PP] Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, registered and certified by Bundesamt fuer Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0084-2014 dated 13 January 2014.

[ST] MF3Dx2 v2, Security Target, Rev. 1.2 dated 17 January 2019.

[ST-lite] MF3Dx2 v2, Security Target Lite, Rev. 1.1 dated 17 January 2019.

[ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).