Certification Report

MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf version 01.1

Sponsor and developer: ***NXP Semiconductors GmbH***
Troplowitzstrasse 20
22529 Hamburg
Germany

Evaluation facility: ***Riscure***
Delftechpark 49
2628 XJ Delft
The Netherlands

Report number:	**NSCIB-CC-175197-CR**
Report version:	**1**
Project number:	**175197**
Author(s):	**Twan van der Schoot/Wouter Slegers**
Date:	**28 January 2019**
Number of pages:	**12**
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-19-175197**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer

NXP Semiconductors GmbH

Business Unit Security & Connectivity

Troplowitzstrasse20, 22529 Hamburg, Germany

Product and assurance level

MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf version 01.1

Assurance Package:

- EAL4

Project number **175197**

Evaluation facility **Riscure 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 EAL4

Validity
Date of 1st issue : **28-01-2019**
Certificate expiry : **28-01-2024**

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

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

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 MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf version 01.1. The developer of the MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf version 01.1 is NXP Semiconductors 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 contactless Security IC provided as an IC hardware platform with an Operating System (OS) and four applications, one per TOE variant.

The TOE is to be used with a Proximity Coupling Device (PCD, also known as terminal) according to the standard ISO14443 Type A. The TOE is primarily designed for secure contactless transport applications, loyalty programs, access management, closed loop payment, account based services and secure NFC applications.

The TOE has been evaluated by Riscure B.V. located in Delft, The Netherlands. The evaluation was completed on 23 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 MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf version 01.1, 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 MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf version 01.1 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 EAL4 assurance requirements for the evaluated security functionality.

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 MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf version 01.1 from NXP Semiconductors GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	Analog	Version A1 dated 15.03.2018
	Digital	Version A1 dated 15.03.2018
Software	Firmware / OS	Version A1 dated 15.03.2018
	Application data	Version A1 dated 15.03.2018

To ensure secure usage a set of guidance documents is provided together with the **MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf version 01.1.** Details can be found in section “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, section 1.4.4.

2.2 Security Policy

The TOE is a contactless Security IC provided as an IC hardware platform with an Operating System (OS) and four applications, one per TOE variant.

The TOE is to be used with a Proximity Coupling Device (PCD, also known as terminal) according to the standard ISO14443 Type A. The TOE is primarily designed for secure contactless transport applications, loyalty programs, access management, closed loop payment, account based services and secure NFC applications.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

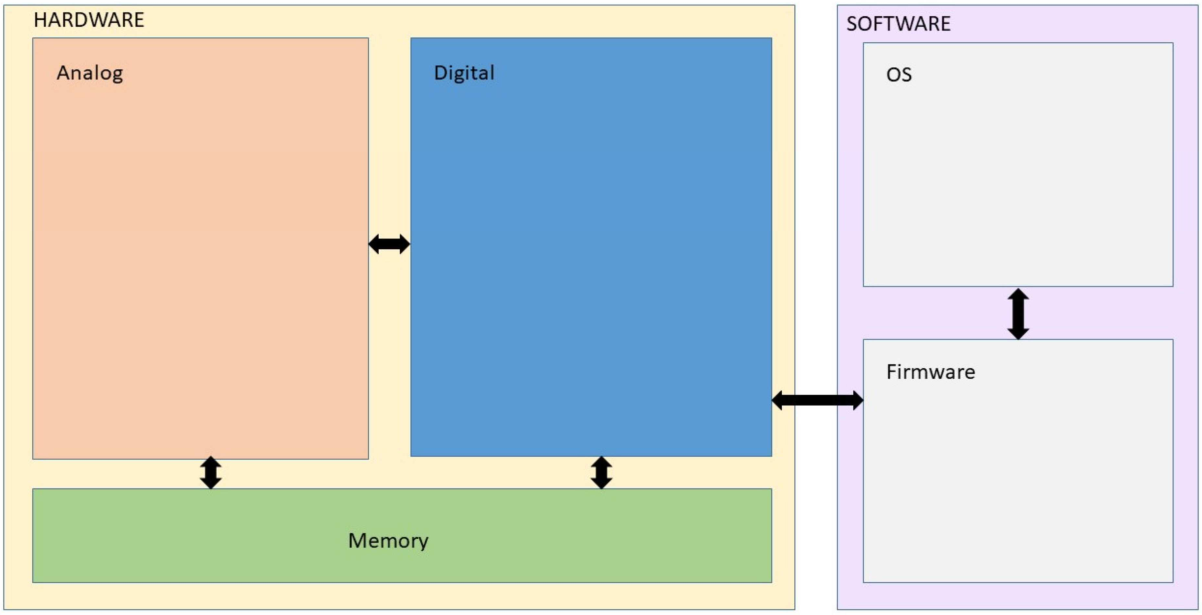
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 4.2 of the *[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 system design decomposes the TOE into three subsystems: Operating System (OS), Firmware and Hardware, as shown in the figure below.



The TOE has two types of TSFIs: physical and logical. There are two physical TSFIs, and 42 logical TSFIs - 34 logical native commands and 8 logical ISO 14443A commands. Detailed information about the logical TSFIs can be found in the TOE datasheets.

Physical TSFIs do not have public documentation as they require no interaction from the user; they are actively monitoring the conductivity of wires. The status of these monitoring activities is observable via the logical TSFIs.

2.5 Documentation

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

Identifier	Version
MF2DL(H)x0 - Information on Guidance and Operation, Guidance and Operation Manual	447910 dated 23.10.2018
MF2ID(H)10 - Information on Guidance and Operation, Guidance and Operation Manual	448010 dated 23.10.2018
NT4H2x21Gf - Information on Guidance and Operation, Guidance and Operation Manual	448111 dated 14.11.2018
NT4H2x21Tf - Information on Guidance and Operation, Guidance and Operation Manual	448211 dated 14.11.2018
MF2DL(H)x0 - MIFARE DESFire Light contactless application IC, Product Data Sheet	430712 dated 05.11.2018
MF2ID(H)10 - MIFARE IDentity – Smart Credential for Account Based Services, Product Data Sheet	465612 dated 05.11.2018
NT4H2421Gx - NTAG 424 DNA – Secure NFC T4T compliant IC, Product Data Sheet	465411 dated 13.11.2018
NT4H2621Gx - NTAG 426 DNA – Secure NFC T4T compliant IC, Product Data Sheet	510310 dated 13.11.2018
NT4H2421Tx - NTAG 424 DNA TT - Secure NFC T4T compliant IC with Tag Tamper feature, Product Data Sheet	465511 dated 13.11.2018
NT4H2621Tx - NTAG 426 DNA TT - Secure NFC T4T compliant IC with Tag Tamper feature, Product Data Sheet	510410 dated 13.11.2018

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 modules (beyond EAL4 requirements). The testing was largely automated using industry standard and proprietary test suites. Test scripts were extensively used to verify that the functions return the expected values.

For the testing performed by the evaluators, the developer has provided samples and a test environment. The evaluators have 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 is performed based on the structure of the attack methods defined by JHAS. For each attack method, the evaluator has analysed and described the objective of the attack and how the attack method applies to the TOE.

2.6.3 Test Configuration

The TOE has four different variants: MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf. As agreed with the certifier, the evaluator performed the tests on the MF2DL(H)x0 variant because it is the TOE variant that supports the largest number of TSFIs (32 out of 34).

The testing results apply to all variants.

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.

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, by use of 11 site certificates (NXP Hamburg, NXP Gratkorn, NXP Bangalore, NXP Nijmegen, SSMC Singapore, ATBK Thailand, CHIPBOND Taiwan, Toppan, NXP Eindhoven, NXP Leuven, and HTC60.

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 **MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf version 01.1**.

The TOE can be identified by using the command Cmd.GetVersion and by a ROM code identifier embedded in metal layer 5 of the TOE.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references a ASE Intermediate Report and other evaluator documents.

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

Based on the above evaluation results the evaluation lab concluded the **MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf version 01.1**, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

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. 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.

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: AES based Leakage Resilient Primitive (LRP).

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

3 Security Target

The MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf Security Target, Revision 1.9, NXP Semiconductors, dated 2018-11-28 *[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
DES	Data Encryption Standard
DFA	Differential Fault Analysis
EMA	Electromagnetic Analysis
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
LRP	AES based Leakage Resilient Primitive
MAC	Message Authentication Code
NFC	Near Field Communication
NSCIB	Netherlands scheme for certification in the area of IT security
OS	Operating System
PCD	Proximity Coupling Device
PP	Protection Profile
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 for MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf version 01.1, Version 1.4, 10 January 2019.

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

[ST] MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf Security Target, Revision 1.9, NXP Semiconductors, dated 2018-11-28.

[ST-lite] MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf Security Target Lite, Rev. 1.0, dated 2018-12-31.

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

(This is the end of this report).