Certification Report

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

Sponsor and developer: ***NXP Semiconductors Germany GmbH***
Beiersdorfstraße 12
22529 Hamburg
Germany

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

Report number:	**NSCIB-CC-2300128-01-CR**
Report version:	**1**
Project number:	NSCIB-**2300128-01**
Author(s):	**Jordi Mujal**
Date:	**27 December 2023**
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.

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 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 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 Security IC comprising a hardware platform, a fixed software package implemented in ROM and a set of data files stored in EEPROM. The software is stored in ROM and provides an operating system which implements a set of functions used to manage various kinds of data files stored in the non-volatile EEPROM memory. The operating system provides access control if required by the configuration. The operating system is designed as platform, which supports command sets for four different applications forming four different product variants.

The TOE was previously evaluated by Riscure B.V. located in Delft, The Netherlands and was certified under the accreditation of TÜV Rheinland Nederland on 28 January 2019 (CC-19-175197). The current evaluation of the TOE has also been conducted by Riscure B.V. and was completed on 27 December 2023 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]*.

There are no changes in the TOE compared from previous evaluations.

The certification took into account that 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 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]* (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 MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf, Version 01.1 from NXP Semiconductors Germany 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. For details, see section 2.5 “Documentation” of this report.

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

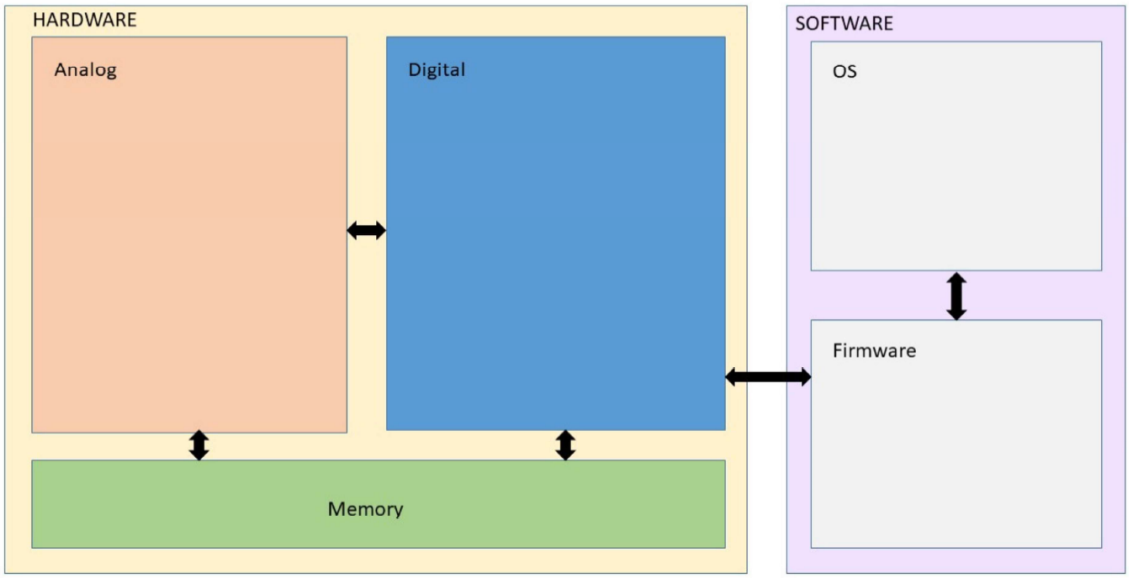
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

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

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 performed extensive testing on functional specification, subsystem and module level (beyond EAL4 requirements). 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 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.

The total test effort expended by the evaluators during this re-evaluation was 5 weeks. During that test campaign, 40% of the total time was spent on Perturbation attacks and 60% on side-channel testing.

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]*. The evaluator concluded that the tests results apply to all TOE variants.

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.

2.7 Reused Evaluation Results

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 multiple site certificates and Site Technical Audit Reports.

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.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an 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 “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: AES based Leakage Resilient Primitive (LRP)

3 Security Target

The MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf Security Target, Revision 1.9, 28 November 2018 *[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
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
LRP	AES based Leakage Resilient Primitive
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 01.1, 20220597-D1, version 2.2, 5 December 2023.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf Security Target, Revision 1.9, 28 November 2018
[ST-lite]	MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf Security Target Lite, Revision 1.0, 31 December 2018
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)