Version 2023-11

Certification Report

MF3E(c)x3

Sponsor and developer:	***NXP Semiconductors Germany GmbH*** **Beierdorfstrasse 12** **22529 Hamburg** **Germany**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-2300018-01-CR**
Report version:	**1**
Project number:	NSCIB-2300018-01
Author(s):	**Andy Brown**
Date:	**26 October 2024**
Number of pages:	**12**
Number of appendices:	**0**

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

® TrustCB is a registered trademark. Any use or application requires prior approval.

CONTENTS

® TrustCB is a registered trademark. Any use or application requires prior approval.

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.

® TrustCB is a registered trademark. Any use or application requires prior approval.

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.

® TrustCB is a registered trademark. Any use or application requires prior approval.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the MF3E(c)x3. The developer of the MF3E(c)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.

NXP has developed the MF3E(c)x3 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. Alternatively, in specific configurations the MF3E(c)x3 can be used with a host MCU through the I2C interface. The MF3E(c)x3 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. It fully complies with the requirements for fast and highly secure data transmission, flexible memory organisation and interoperability with existing infrastructure.

The TOE is a smart card IC comprising a hardware platform and a fixed software package. The software package is stored in 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 32-bit CPU, volatile and non-volatile memories, cryptographic coprocessors, security components and two communication interfaces.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 26 October 2024 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 MF3E(c)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 MF3E(c)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 EAL6 augmented (EAL6+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ASE_TSS.2 (TOE Summary Specification).

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.

® TrustCB is a registered trademark. Any use or application requires prior approval.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the MF3E(c)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	MF3E(c)x3 Hardware	B0
IC Dedicated Test Software	Test Software	3.0.11
IC Dedicated Support Software	Boot Software	3.0.11
	Firmware	3.0.11
	Crypto Library	2.4.2
	Operating System	3.0.1

To ensure secure usage a set of guidance documents is provided, together with the MF3E(c)x3. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.4.3

2.2 Security Policy

The TOE has the following features as listed in *[ST]*:

- Flexible file system that groups user data into applications and files within each application
- Support for different file types like Data files, Value files, Record files, including definition of multiple file access conditions per file
- ECC-based Mutual and Reader-Unilateral Authentication
- ECC-based Card-Unilateral Authentication and generic ECDSA support
- AES-based Mutual Authentication and Secure Messaging (EV2 Secure Messaging)
- Authentication on application level with fine-grained access conditions for files
- Multi-application support that allows distributed management of applications and ensures application segregation
- Delegated-application support that allows third party service providers to create their applications onto the issued TOE
- Multiple application selection that allows transaction over files in two applications
- Data encryption on the communication path
- Message Authentication Codes (MAC) for replay attack protection
- Flexible key management (for symmetric and asymmetric keys) on PICC and application level
- ECC keypair generation
- Transaction system with rollback that ensures consistency for complex transactions
- Unique serial number for each device (UID) with optional random UID
- Key set rolling feature per application to switch to a predefined symmetric key set

® TrustCB is a registered trademark. Any use or application requires prior approval.

- Transaction MAC feature (via AES-based CMAC or ECDSA signature) to prevent fraudulent merchant attacks
- ECC-based originality functionality that allows verifying the authenticity of the TOE
- Proximity check feature for protection against relay attacks on the TOE
- Secure Dynamic Messaging feature which allows confidential (via AES-based encryption) and integrity protected data (via AES-based CMAC or ECDSA signature) exchange without requiring a preceding authentication

If privacy is an issue, the TOE can be configured not to disclose any privacy-related information to unauthorized users.

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 5.2 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 CPU of the MF3E(c)x3 has a 32-bit architecture. The on-chip hardware components are controlled by the software via Special Function Registers. These registers are correlated to the activities of the CPU, the memory protection unit, interrupt control, contactless communication, Flash, timers, the AES co-processor and the ECC co-processor. The communication with the MF3E(c)x3 can be performed through the contactless interface or in specific configurations using the I2C interface.

The ECC co-processor supports ECC operations with a key length of 256 bit over the NIST P-256 and brainpoolP256r1 curves. The AES co-processor supports AES operations with a key length of 128 and 256 bit.

A hardware Random Number Generator provides true random numbers which are used to seed deterministic random number generators, used internally by the operating system for security purposes.

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 TOE also contains IC Dedicated Support Software. The Boot Software which is stored in ROM is part of the IC Dedicated Support Software. This software is executed after each reset of the TOE, i.e. every time when the TOE starts. It sets up the TOE and does some basic configuration. The operating system is also part of the IC Dedicated Software and provides the main functionality of the TOE in the usage phase. The MF3E(c)x3 is primarily designed for secure contactless transport applications and related loyalty programs as well as access control systems. It fully complies with the requirements for fast and highly secure data transmission, flexible memory organization and interoperability with existing infrastructure.

2.5 Documentation

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

® TrustCB is a registered trademark. Any use or application requires prior approval.

Identifier	Version
MF3E(c)x3, Information on Guidance and Operation, User manual	1.2
MF3E(H)x3, MIFARE DUOX contactless smartcard IC, Product data sheet	1.0
MF3E(H)x3 PDC, MIFARE DUOX Post Delivery Configuration, Preliminary data sheet addendum	0.1
MF3E(c)x3, Wafer and delivery specification, Product data sheet addendum	1.2

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 tests cover all security functions and aspects of the TSF. The developer used a set of test suites (mostly proprietary and compatibility ones) and tools to test the TOE. Since the TOE consists of hardware and software components, each component is tested using specific test suites.

The OS was fully covered by unit testing. The Crypto Library was tested through the OS API. The HW/FW of the TOE was covered by unit testing. This is complemented by end-to-end tests on TSFI level (OS API), testing all relevant functionality on the actual TOE hardware thereby providing assurance that the complete TOE was functioning properly (including the HW and the FW).

The developer used the TOE in SO28 or White Card package as well as Software simulators and FPGA tool when some tests could only be performed in such environment. To further support the hardware, component testing was used that verified several aspects (e.g. return values, registers, CPU and others) in an automated manner. These tests are complemented by code inspection and code coverage analysis done by the developer.

The developer used a distributed test environment to allow usage of a vast amount of simultaneously driven testing equipment where results are logged automatically in XML/HTML-based files.

The tests were grouped in a number of categories including positive/negative tests, functional acceptance or functional destructive tests, functional tests and non- functional tests.

The developer has performed extensive testing on FSP, subsystem, module and module interface level. The tests were performed by the developer through execution of the test scripts using an automated and distributed system. Test tools and scripts were extensively used to verify that the tests return expected values. The identification was checked using tools to verify identification and versions of the TOE Hardware and TOE software.

Code coverage analysis was used by the developer to verify overall test completeness. Test benches for the various TOE parts were executed using code coverage measurement and analysis tools to determine the code coverage (i.e. lines, branches and/or instructions, depending on tool) of each test bench. Cases with incomplete coverage were analysed. For each tool, the developer has investigated and documented inherent limitations that can lead to coverage being reported as less than 100%. In such cases the developer provided a “gap” analysis with rationales (e.g. attack counter not hit due to redundancy checks).

The ATE evaluation approach is based on code coverage analysis. The evaluator also used an acceptable alternative approach (as described in the application notes, Section 14.2.2 in *[CEM]*) and used analysis of the implementation representation (i.e. inspection of source code) to validate the rationales provided by the developer.

In addition, the evaluator created additional test cases to confirm verification of the version of the TOE / to supplement coverage of SFRs and/or TSFI / to further exercise the behaviour of critical functionality.

® TrustCB is a registered trademark. Any use or application requires prior approval.

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. This analysis was performed according to the attack methods in section 5 of *[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.

The total test effort expended by the evaluators was 17 weeks. During that test campaign, 35% of the total time was spent on Perturbation attacks, 60% on side-channel testing, and 5% on logical tests.

2.6.3 Test configuration

The configuration of the sample was the same as described in the *[ST]*. Some tests were performed in earlier versions of the firmware. Additional work in ADV and AVA concluded that changes did not affect the testing results.

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

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 25 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 MF3E(c)x3.

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 MF3E(c)x3, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 6 augmented with ASE_TSS.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]*.

® TrustCB is a registered trademark. Any use or application requires prior approval.

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: **None**

® TrustCB is a registered trademark. Any use or application requires prior approval.

3 Security Target

The MF3E(c)x3 Security Target, Revision 1.3, 03 September 2024 *[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

® TrustCB is a registered trademark. Any use or application requires prior approval.

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 “NXP MF3E(c)x3” – EAL6+, 24-RPT-1100, Version 1.0, 26 September 2024

[JIL-AAPS] JIL Application of Attack Potential to Smartcards, Version 3.2, November 2022

[JIL-AMS] 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 2.6, 02 August 2022

[PP] Security IC Platform Protection Profile with Augmentation Packages, registered under the reference BSI-CC-PP-0084-2014, Version 1.0, 13 January 2014

[ST] MF3E(c)x3 Security Target, Revision 1.3, 03 September 2024

[ST-lite] MF3E(c)x3 Security Target Lite, Revision 1.0, 09 September 2024

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

(This is the end of this report.)

® TrustCB is a registered trademark. Any use or application requires prior approval.