MIFARE DESFire EV1/EV2

Protection Profile

1.0 — 20 December 2018 **Specification**

information

Info	Content
Keywords	Common Criteria, Protection Profile, Security, Evaluation, Certification
Abstract	This document describes the security problem definition, security objectives and security requirements to be considered when either a MIFARE DESFire EV1 or MIFARE DESFire EV2 compliant technology is implemented.

Revision history

Rev	Date	Description
0.1	20180312	First Release
0.2	20180316	Removal of MIFARE PLUS references
0.3	20180520	Version for discussion with stakeholders
0.4	20180720	Version for trial use
1.0	20181220	Version for formal use in MIFARE scheme v3.0

Contact information

For more information, please visit: http://www.nxp.com

For sales office addresses, please send an email to: salesaddresses@nxp.com

1. PP Introduction

NXP, the scheme owner of the MIFARE scheme and manager of the risks to MIFARE systems and the MIFARE brand, decided that this PP describes the required assurance for a CC evaluation of the DESFire EV1/EV2 products by applying CC in a smart manner.
This PP describes the requirements on TOEs implementing MIFARE DESFire EV1/EV2: the security function policy (MIFARE SFP) encoded in this PP is to enforce the [MIFARE-DES-EV1]/[MIFARE-DES-EV2] protocols and their access control in the MIFARE services, even in the face of a state-of-the-art attacker.

1.1 PP Reference

"MIFARE DESFire EV1/EV2 Protection Profile", version 1.0.

1.2 TOE Introduction and type

The TOE is a smart card or similar device, comprising of a hardware platform and embedded software, providing MIFARE DESFire EV1/EV2 functionality.

1.3 Required non-TOE hardware/software/firmware.

The TOE requires an ISO 14443 card terminal to be provided with power and to receive adequate commands.

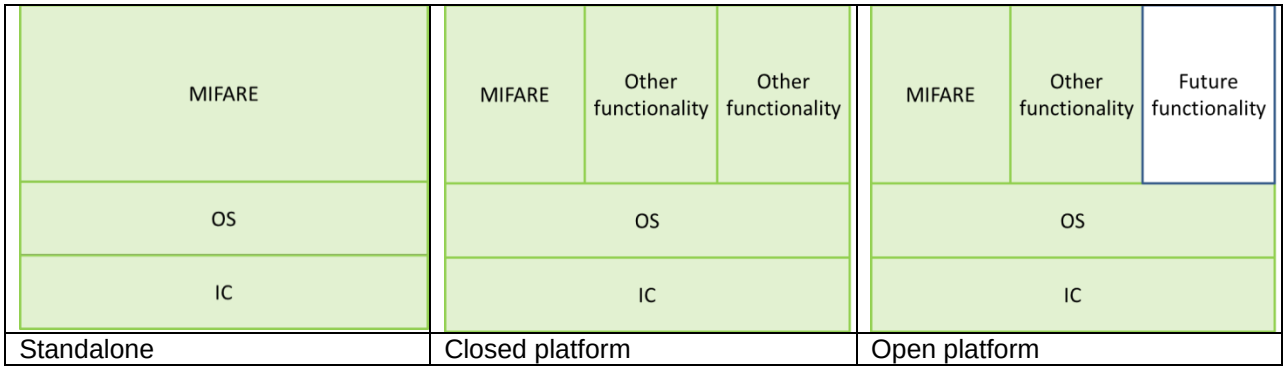
1.4 TOE Description

1.4.1 Physical scope of the TOE

The TOE physically consists of a smart card IC or similar device.

1.4.2 Logical scope of the TOE

The TOE logically consists of the smart card IC (EMVco or CC PP-0084 [PP84] certified, or inside this scheme) and embedded software.



If only MIFARE functionality is available, the TOE is said to be "standalone".
If the TOE is not standalone, i.e. other functionality such as a payment application is available, the potential impact of this non-MIFARE functionality on the MIFARE functionality must be analyzed.
If all functionality is already in the scope considered during the evaluation, the TOE is said to be "closed platform".
If there is the possibility to add any other functionality (such as other applications) beyond the scope considered during this evaluation, the TOE is said to be "open platform".
Application note: the ST shall identify which of the mentioned designs applies to the TOE.

Application note: the ST shall identify which MIFARE specifications ([MIFARE-DES-EV1]/[MIFARE-DES-EV2]) the TOE conforms to. This specific MIFARE specification is referred to as “MIFARE specification” in the remainder of this PP.
Application note: the ST shall identify all CC/EMVco certified components (at least the hardware, possibly any crypto libraries and JavaCard OSs), including identification of the component, certification identifier and date of certificate issuance.

1.4.3 Life-Cycle scope

The TOE is delivered to a (pre-)personalizer, and eventually to the end user. The TOE is in the evaluated configuration after personalization.

2. Conformance Claims

2.1 CC Conformance claim

This Protection Profile claims to be conformant to the Common Criteria version 3.1, Revision 5. It is CC part 2 and part 3 conformant.

2.2 PP Claim

This Protection Profile requires strict conformance for any ST or PP claiming conformance to this PP.
Application note: no additional SFRs or SARs beyond those from other MIFARE PPs may be claimed under the MIFARE scheme.

2.3 Package Claim

This PP claims the EAL4 assurance package, augmented with AVA_VAN.5 and ALC_DVS.2.

2.4 PP Application notes

The application notes and refinements for assurance requirements of the common smartcard assurance package of EAL4-EAL6 augmented with AVA_VAN.5 and ALC_DVS.2 are included in this PP, and should be used for evaluations under the MIFARE scheme.

3. Security Problem Definition

3.1 Threat

An attacker with high attack potential and with physical and logical access to the TOE and its interfaces, is able to perform an operation that is not allowed in accordance to the applicable MIFARE specifications.
Application note: compromises of one or more of the assets described in the related MIFARE Security Analysis ([MIFARE-SA-DF] for the MIFARE DESFire EV1/EV2)[1] is considered sufficient to mount such a successful attack and hence fail the evaluation.

3.2 Policy

Production and personalization sites should fulfill the MIFARE Robustness requirements.

3.3 Assumption

There are no assumptions.

[1] Due to its sensitivity, this document is only made available to the necessary parties by the Scheme Owner.

4. Objectives

4.1 Objective for the TOE

The TOE shall implement the MIFARE specification exactly, robust against a high attack potential attacker. This counters the threat identified.

4.2 Objective for the Environment

The TOE production and personalization sites should fulfill the MIFARE Robustness requirements [MIFARE-DES-Robustness] and [MIFARE-DES-Robustness-Post-issuance]. This fulfills the policy described earlier.

5. Extended Components Definition

None.

6. Security Requirements

6.1 Security Functional Requirements

6.1.1 FDP_ACC.2 Complete access control

Hierarchical to: FDP_ACC.1 Subset access control
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1
The TSF shall enforce the MIFARE SFP[2] on external entities accessing the TOE[3] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2
The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

6.1.2 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1
The TSF shall enforce the MIFARE SFP[4] to objects based on the following: currently authenticated service and requested operation[5].

FDP_ACF.1.2
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: MIFARE specification allows the operation[6].

FDP_ACF.1.3
The TSF shall explicitly initialize access of subjects to objects based on the following additional rules: none[7]

1. [2] [assignment: access control SFP]
2. [3] [assignment: list of subjects and objects]
3. [4] [assignment: access control SFP]
4. [5] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]
5. [6] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
6. [7] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

FDP_ACF.1.4
The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[8].

6.1.3 FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1
The TSF shall enforce the MIFARE SFP[9] to provide restrictive[10] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2
The TSF shall allow ~~the~~[11] none[12] to specify alternative initial values to override the default values when an object or information is created.

6.1.4 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1
The TSF shall enforce the MIFARE SFP[13] to restrict the ability to *query, modify, delete*[14] the security attributes listed in the MIFARE specification[15] to users as specified in the MIFARE specification[16].

6.1.5 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No dependencies.

FMT_SMF.1.1
The TSF shall be capable of performing the following management functions: query, modify, delete as described in the MIFARE specification[17].

6.2 Security Assurance Requirements

EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.

6.3 Rationale

All SFRs map to the objective for the TOE, starting with FDP_ACC.2 and FDP_ACF.1, and then including the dependencies as described below.

7. [8] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
8. [9] [assignment: access control SFP, information flow control SFP]
9. [10] [selection, choose one of: restrictive, permissive, [assignment: other property]]
10. [11] refinement
11. [12] [assignment: the authorised identified roles]
12. [13] [assignment: access control SFP(s), information flow control SFP(s)]
13. [14] [selection: change_default, query, modify, delete, [assignment: other operations]]
14. [15] [assignment: list of security attributes]
15. [16] [assignment: the authorised identified roles]
16. [17] [assignment: list of management functions to be provided by the TSF]

6.3.1 Dependencies

The dependencies are satisfied as follows:

SFR	Dependencies	Satisfied
FDP_ACC.2	FDP_ACF.1	Yes: In PP
FDP_ACF.1	FDP_ACC.1	Yes: In PP
	FMT_MSA.3	Yes: In PP
FMT_MSA.3	FMT_MSA.1	Yes: In PP
	FMT_SMR.1	Yes: In PP
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	Yes: FDP_ACC.2 in PP (hierarchical to FDP_ACC.1)
	FMT_SMR.1	Refined away: there is only one role and it is spelled out in FMT_MSA.1
	FMT_SMF.1	Yes: In PP
FMT_SMF.1	No dependencies	Not applicable

7. Application notes

NXP, the scheme owner of the MIFARE scheme and manager of the risks to MIFARE systems and the MIFARE brand, decided that for evaluations against this PP, the following application notes shall be applied.

7.1.1 Application note ASE

The MIFARE scheme provides a ST template that should be used and fulfills the ASE requirements efficiently.
The TOE identification must include a clear and explicit reference to the identification method.
The identification method shall be clearly and completely described to the customers of the product, and shall be sufficiently practical to be applied by the customer and any entity determining whether a product is the evaluated product when a product is taken from the field.
The method of identification may consist of several identification steps. For example, the verification of the hardware part may differ from the verification of the software parts.
Note that this method of product identification shall be used to verify the platform identifier during any subsequent composite activity, and in situations where it is contested that a product found in the field is the evaluated product.
The evaluator shall determine that the product identification is consistent with the product identification method. The evaluator shall determine that any underlying platform identification steps relevant for the product identification are performed or consistently communicated to the user of the product as needing to be verified.
The evaluator shall verify that the samples can be used according to the TOE identification method. Any divergence for testing purposes (such as test patches or configuration settings) must be documented in the ETR, including an analysis why this has no negative impact on the assurance gained.
As per application note, the Security Target should also identify which of the TOE designs is applicable.
The evaluator shall report this verification with a simple statement in the ETR.

7.1.2 Application note AGD

The preparative guidance listed in the ST should be considered together with the MIFARE specifications. No operational guidance other than the MIFARE specifications is allowed. If only the MIFARE specification is referred to for preparative/operational guidance, the evaluator and certifier should consider the MIFARE specifications to fulfill the requirements of AGD_PRE.1 and AGD_OPE.1 respectively. The evaluator shall check that the preparative guidance, executed by experienced personalizers, is clear and leads to the TOE as tested by the evaluator. The evaluator shall report this verification with a simple statement in the ETR.

7.1.3 Application note ADV_FSP up to ADV_FSP.5

The MIFARE specification and the standards such as ISO 14443 and the Java Card Specs it refers to, are the sole and complete specification of the functionality of the MIFARE part of the TOE.
The evaluators should verify that no other specification is referred to by the developer. No other specification shall be deemed relevant by the evaluators. If only the MIFARE specification and ISO 14443 is referred to, the evaluator and certifier should consider the requirements of ADV_FSP to be fulfilled as all are industry standards well known to meet these requirements.
The evaluator shall report this verification with a simple statement in the ETR.

7.1.4 Application note ADV_TDS up to ADV_TDS.5

As the functionality and reasonable designs of this type of TOE are limited, the design is expected to be one of the identified general designs described above in the TOE scope in the TOE Description section. With this information, and the facts that the functional specification is complete, the functional testing is comprehensive, and the underlying platform is CC or EMVco certified, the evaluators have sufficient information to understand the TOE to perform their ADV_IMP code review and AVA vulnerability analysis.
The evaluator shall verify, as part of the ADV_IMP activities, that the source code fits the general design as described above.
If the source code fits the design as described above and the evaluator can perform the ADV_IMP activities with little confusion on the structure of the TOE, the requirements of ADV_TDS are considered fulfilled (as allowed under “Collection of Developer evidence”).
The evaluator shall report the verification that the source code fits the general design with a simple statement in the ETR.

7.1.5 Application note ADV_ARC

If the TOE is a platform, the TOE must protect the MIFARE assets against any other application.
If the TOE is a closed platform, this may be determined by analysis of the other applications or analysis of any mechanisms separating the applications.
If the TOE is an open platform, the mechanism separating the applications shall be considered.
A certified JavaCard platform should be considered to sufficiently provide such separation.
The evaluator should gather the understanding of the security architecture during the ADV_IMP activities (as allowed under “Collection of Developer evidence”).
The evaluator shall report this understanding of the security architecture in a short summary in the ETR.

7.1.6 Application note ADV_IMP

During the code review, the evaluator shall also verify that:

- The code matches the standard design identified in the ST.

- The MIFARE functional testing will exercise all relevant code paths and behaviour of the TOE. This may be determined by code review, code coverage tools, or other means.
- All relevant guidance of the underlying platform (hardware, any crypto libraries, any OS) is applied.
- The scope of the evaluation of the underlying platform includes at least AES, DES and RNG functionality, and in the case of an open platform separation between the applications and the MIFARE functionality.

The evaluator shall report this verification with a simple statement in the ETR.

7.1.7 Application note ATE

The MIFARE functional testing is mandatory for all licensees. The evaluator and certifier shall consider the MIFARE Functional Certification (functional testing) to fulfill the requirements of ATE_COV (as the testing is complete on the interfaces), ATE_FUN (as the testing is completed and passed), and ATE_IND (as the testing is performed completely there is no useful additional functional test, and as the testing is performed by independent testers already there is no useful additional independent testing).
The evaluator shall report the MIFARE Functional Certification ID in the ETR.

The evaluator shall determine in ADV_IMP that the MIFARE functional testing exercises all relevant behavior of the TOE, considering especially whether there are execution paths unlikely to be exercised. The evaluator and certifier shall consider this to fulfill the requirements of ATE_COV and ATE_DPT.
The evaluator shall report the result of this check with a simple statement in the ETR.

7.1.8 Application note ALC_LCD/ALC_CMC/ALC_CMx/ALC_DVS/ALC_DEL

The development and production life-cycle is expected to follow the [PP84] life cycle. The intention is to ensure that all sites involved in the development and production of the product, including all underlying hardware and platform components, have been audited to protect the integrity and confidentiality of the product against any attacker having a high attack potential. It is expected that all sites have already undergone equivalent site audits. Therefore, these audits should be re-used.
The developer shall deliver an overview of the sites involved in the development and production of the product. The overview shall summarize the sites, their role, the Common Criteria or EMVCo certification ID under which the Site Audit has been performed shall also be provided for each site, as well as the date of the last audit. Sites may be re-used on the basis of both site and product certifications.
The evaluator shall confirm that it has received a declaration from the developer that all identified sites:

- Are still operating in a manner compatible with the site audit scope and passing verdicts.
- Are used for the development or production of this product in a manner that is consistent with the site audit scope.
- Confirms that the site security and configuration management requirements applied during the site audit provide sufficient assurance for the integrity, authenticity and confidentiality of the MIFARE design information and TOE.

The evaluator shall verify from the provided overview whether the described combination of sites is consistent with the evaluation evidence provided. The evaluator shall also verify whether the combination of sites together is likely able to develop and produce the complete product securely. The evaluator shall verify that all audits are at most 2 years old. If these aspects are met, the assurance requirements of ALC_LCD, ALC_CMC, ALC_DVS and ALC_DEL are met.

The evaluator shall report this verification with an overview of the sites, their role, the applicable audit report and validity date, and a statement that the evaluator has verified that the combination of sites together is likely able to develop and produce the complete product securely.

7.1.9 Application note AVA

The evaluator's vulnerability analysis shall use the relevant MIFARE security analysis for the definition of the assets and for a minimum set of possible attacks to be considered. Rating shall be done according to the latest version of JIL Application of Attack Potential to Smartcards [AM] and JIL Attack Methods for Smartcards and Similar Devices [AP]. The evaluator shall report his analysis, including the versions of the MIFARE security analysis, JIL Application of Attack Potential and JIL Attack Methods for Smartcards and Similar Devices in the ETR.

8. Rationales

The objective for the TOE directly follows from the security problem definition.
A TOE implementing the MIFARE specifications exactly will meet the objective for the TOE, hence the SFRs encode this.
The SARs are chosen to meet the minimum requirements for this kind of TOE.

8.1 Reference Materials

The documents listed in Table 1 may have been cited in this document or used to obtain background information.

Table 1. Reference Documents

Title	Source	Reference
MIFARE DESFire EV1 Interface Specification, Rev. 1.1 (ts335111)	4	[MIFARE-DES-EV1]
MIFARE DESFire EV2 Reference Architecture, Rev. 1.4 (ra321914)	4	[MIFARE-DES-EV2]
MIFARE DESFire EV2 Compliance and Robustness Rules, Rev 1.1 (sp284811)	4	[MIFARE-DES-Robustness]
MIFARE DESFire EV2 Compliance and Robustness Rules supporting post-issuance use case, Rev 1.1 (sp284711)	4	[MIFARE-DES-Robustness-Post-issuance].
MIFARE Security Analysis MIFARE DESFire	4	[MIFARE-SA-DF]
EUROSMART Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, version 1.0.	5	[PP84]
Joint Interpretation Library Application of Attack Potential to Smartcards, version 2.9, dated January 2013	6	[AP]
Joint Interpretation Library Attack Methods for Smartcards and Similar Devices, version 2.2, dated January 2013	7	[AM]

Key:

1 = Available online from the Joint Interpretation Library

2 = Available from the ISO standards website (www.iso.org)

3 = Available via Internet http://emvco.com

4 = Available via Internet https://www.docstore.nxp.com

5 = Available via Internet https://www.commoncriteriaportal.org/

6 =Available via Internet https://sogis.org/

7 = Available via JHAS membership

[This page is intentionally left blank.]

9. Legal information

9.1 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information.

NXP Semiconductors is not responsible for the testing and/or approval and In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related thereto, whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Licensee understands that approval in accordance with this Security Evaluation Scheme does not constitute a recommendation for use of the product nor is it a guarantee that the product is totally free of any exploitable vulnerability. There is always a residual probability that exploitable vulnerabilities have not been discovered.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the Licensee's applications or products, or the application or use by Licensee's third party customer(s). Licensee is responsible for doing all necessary testing for the Licensee's applications and products in order to avoid a default of the applications and the products or of the application or use by Licensee's third party customer(s). NXP does not accept any liability in this respect.

9.2 Export control — **This document may be subject to export control regulations. Export might require a prior authorization from competent authorities.**

9.3 Trademarks

Notice: All referenced brands, product names, service names and trademarks are property of their respective owners.

MIFARE, MIFARE Plus MIFARE DESFire — are trademarks of NXP B.V.

10. List of figures

No table of figures entries found.

11. List of tables

12. Contents

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 20 December 2018