MIFARE Security Evaluation Scheme

Application Form and Guidance Notes

Rev. 2.0 — 9 December 2016 **Scheme Application Form**

Document information

Info	Content
Keywords	MIFARE, Security, Evaluation, Certification
Abstract	Application form and Guidance Notes for the MIFARE Security Evaluation Scheme

1. Document Usage

The **NXP MIFARE Security Evaluation Scheme** is used by NXP to demonstrate that a specific product is in compliance with the security requirements associated with either the MIFARE Plus® or MIFARE DESFire ® Products.

In order to initiate the Security Evaluation Process the licensee must first fill out the **L**icensee **S**ubmission **F**orm (section 2 below) included in this document. Sections 3 and 4 of this document are intended to provide guidance on the information that NXP expects this completed form to contain.

1.1 Audience

This document is restricted to use by authorized personnel of the following involved parties:

1. Licensee: develop the Test Subject
2. NXP acting as an administrative entity: record the Test Subject and give administrative numbers
3. NXP approved Security Laboratory: verify the security level of the Test Subject
4. NXP approved Certification Authority: approve the Test Subject

The MIFARE Licensees apply for a certificate from this evaluation scheme.

1.2 Submission Procedure

This document is distributed in PDF format as an electronic form by NXP to applicants as a result of an enquiry to MIFARE Certification. This document may have some administrative fields pre-filled by NXP for the convenience of the applicant. It is designed to be used with Adobe Acrobat Reader. Fields are highlighted and text can be entered and dropdown selections made. All fields are designed to be visible and wrapped for convenient and accurate printing. The document must be signed by the responsible person.

Digital Signing

On completion the document can be digitally signed by clicking on the sign field by the responsible person. The system will prompt for this. If the applicant does not have a digital signature file then they can create one using the Adobe Security Settings, Add Digital ID option in Acrobat Reader. Once signing all the fields in the form are locked. The next step is to save the document to PDF and giving it a unique name that describes the application.

Manual Signing

As an alternative to digital signing, the applicant may print this document including the form to hardcopy. Then the document may be manually signed and the complete document rescanned to PDF.

The final step is to send this completed document as an email attachment to MIFAREcertification@nxp.com. This will be checked by NXP with feedback within five working days. If the form has been accepted then it will be signed by NXP and returned as a fixed PDF to the applicant. The applicant can then send this information to the approved Security Laboratory or Certification Authority to commence evaluation under the scheme.

If information in this document is changed throughout the MIFARE Security Evaluation the Certification Authority must submit the latest version to NXP along with the MIFARE Certification report for signoff.

2. Licensee Submission Form

Product Registration Number (Assigned by NXP):

Licensee Information	
Licensee Organization Name	
Licensee Primary Contact: (Full Name and Title)	
Telephone Number	
Email address	
Mailing Address	
Street	
City, State	
Country Code	
Date of Submission	

Product Description	
Manufacturer	
Product Name	
Device Form Factor (Smartcard, MicroSD, SIM, sticker, VFBGA…)	
Communication Protocols, Supported	
Platform (Name and version number)	
Platform Main Features	
Platform Security Certificate	
Hardware (Name and version number)	
Hardware Security Certificate	

Product Configuration		
MIFARE Application(s) evaluated(including version numbers)		
Standalone or Integrated MIFARE product		
Configuration to be evaluated (#1 or #2 or #3 or #4)		
Previous Product Registration	Product Registration Number / Approval Reference Number	Changes (if any)
If applicable, provide the registration number of a previously approved product and list changes.		
Supported algorithms (DES, AES, DES and AES)		
Additional applications embedded in the Test Subject	"Additional applications" means applications which are operational before issuance. Applications loaded after issuance must be compliant with security requirements dedicated to the platform	
Does this product contain any applications other than MIFARE Plus, and MIFARE DESFire? If yes, provide a description of each application.	Application Names 1	Description

Do any applications that are not MIFARE Plus or MIFARE DESFire compliant interact in any way with the MIFARE Plus or MIFARE DESFire applications? If yes, provide a description of each application.	Application Names 2	Description

IC Documentation and Information	
Point of Contact	
IC Datasheet	
IC Security Guidelines	
IC Vendor's Cryptography Library Security Guidelines	
Evidence of a valid IC Vendor's Cryptography Library Certificate	

Platform Documentation and Information	
Point of Contact	
Platform Datasheet	
Platform Security Guidelines	

Security Lab and Certification Authority Selection	
Security Lab selected	
Certification Authority selected	

Additional Information	
Any additional relevant information or additional application information may be entered here.	

MIFARE Security Evaluation Conditions

On receipt of a letter of approval and certification report from the certification lab, NXP will, upon request, add the registered product to the approved products list. The letter of approval will testify that the MIFARE product has successfully passed the MIFARE Security Evaluation.

However the following conditions apply:

1) The approval applies only to the specific version and release of the product in its evaluated configuration.
2) The approval 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.
3) You accept that NXP is not responsible for the testing and/or approval and NXP assumes no liability whatsoever related thereto.

By requesting registration you agree to the above conditions.

Name:

Title :

Date:

Signature:

[Signature of a person entitled to engage the company]

NXP Signature

Name:

Title :

Date:

Signature:

[Signature of a person authorized to sign on behalf of NXP]

3. Notes for Guidance

3.1 Document Organization

This section provides general information useful when completing this Licensee Submission Form above and provides an explanation for each section in order to ease the process for the Licensees.

3.1.1 Naming Conventions

The Naming Convention is defined in [MIFARE-SEC].

3.1.2 Terminology

The following terminology applies:

- “shall” or “must” Denotes a mandatory requirement
- “should” Denotes a recommendation
- “may” Denotes an optional feature

3.2 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 Security Evaluation Scheme	1	[MIFARE-SEC]

Key:

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

3.3 Contact Names and Inquiry Procedures related to the security evaluation

All requests or inquiries should be addressed by email to: MIFAREcertification@nxp.com.

4. Submission Form Section Explanations

This section describes the information required in each section of the Licensee Submission Form.

4.1 Product Registration Number

This number will be provided by NXP once the form has been submitted by the Licensee; accordingly this section should be left blank by the licensee when filling in the form.

4.2 Licensee Information

The MIFARE Security Evaluation Scheme is only open to NXP MIFARE Licensees. This section is intended to capture the Licensee information to allow NXP to check the validity of the license and also have the most appropriate contact for the evaluation process.

The information requested in this section is quite straightforward.

4.3 Product Description

The information in this section is intended to provide enough detail to the labs to allow them to assess the scope and complexity of the evaluation. To do this information about the product architecture is required. This will include the underlying IC hardware, including certificate numbers, any platform details (type and certificate numbers) and any additional applications which co-exist on the platform. The configuration which is to be evaluated should also be provided here.

The document **NXP MIFARE – Security Evaluation Scheme** has information on this in section **2.5.2 Configuration** and this should may be referenced for additional guidance.

4.3.1 Manufacturer(s)

This will normally be the name(s) of the Licensee as well as the provider of the underlying platform (where appropriate) and the provider of the Integrated Circuit.

4.3.2 Product Name

This will be the name which appears on the Certificate issued on successful completion of the Evaluation Process and should normally be the commercial name used for the product.

4.3.3 Device Form Factor

Intended to let the laboratories know what package type they will have to handle. Normally this will be one of the following types: Smart Card, SIM, MicroSD, sticker, …

4.3.4 Communication Protocols Supported

For most Smartcard product types this will be ISO/EIC 7816 for contact cards or ISO/IEC 14443 Type A for contactless, however other protocols are possible and it is important to list the ones which the Security Laboratories will have to handle.

4.3.5 Platform

For this first part, if a platform is used, enter the name of the platform and version number.

4.3.6 Platform main features

For instance, Java Card version, GP version, Post-issuance capability…

4.3.7 Platform security certificate

Enter the CC certificate number or PCN number for EMVCo certification.

4.3.8 Hardware

Enter the name of the Integrated Circuit used as well as its version number.

4.3.9 Hardware security certificate

Enter the CC certificate number or ICCN number for EMVCo certification.

4.3.10 MIFARE application(s) evaluated

Normally this would be MIFARE Plus or MIFARE DESFire EV1, but it is possible it could be both and more variants will be available in future. All MIFARE applications that are to be evaluated should be listed here.

4.3.11 Standalone or Integrated MIFARE Product

If there are other applications besides MIFARE residing on the product, then it is considered as an integrated product (and these applications should be listed in a subsequent entry box in this form.) If the only application resident at the time of certification is MIFARE then it is considered as a standalone product. Enter either Standalone or Integrated in this box.

4.3.12 Configuration evaluated

There are two possible configurations to choose from. These are explained in more detail in the Security Evaluation Scheme document, but in summary:

#1: Standalone on Platform

#2: Integrated on Platform (two flavors: Open Platform or Closed Platform)

#3: Standalone on Hardware IC

#4: Integrated on Hardware IC

Choose the configuration which applies to this evaluation.

4.3.13 Previous Product Registration

If this product is based on a product which has already been evaluated under the MIFARE security certification scheme, then please provide the Approval Registration Number and the Product Registration Number if available. Then provide a short description of what the changes are between this product and the one which has been previously evaluated, as this will give more assistance to the labs in determining the testing required.

If there are no previous registered products on which this one is based then please enter Not Applicable, or N/A in the form.

4.3.14 Additional Applications

Please enter any additional applications which are embedded in the test subject. “Additional applications” means applications which are operational before issuance. Applications loaded after issuance must be compliant with security requirements dedicated to the platform. Please list all applications other than MIFARE Plus and

MIFARE DESFire under the heading “Application Names 1” and provide a description of each one in the “Description“ box.

Then, in the “Application Names 2” box list any of these applications which interact in any way with the MIFARE Plus or MIFARE DESFire applications. In the adjoining Description box, please indicate what form the interaction takes.

4.4 IC Documentation and Information

The intention of this section is to allow the labs to gather the necessary information to enable them to determine the scope of testing and to perform the analysis necessary to generate the test plan for the product. So contact details and documentation references are requested for both the Integrated Circuit on which the product is based as well as any platform details which may be relevant.

4.4.1 Point of contact

Please enter the main contact for information on the IC. This should be someone with access to all relevant security certification information for the IC.

4.4.2 IC Datasheet

Please provide the datasheet reference including version number for the IC.

4.4.3 IC Security Guidelines

Please provide the reference including version number for the guidance documentation which is required for the underlying security certification of the IC.

4.4.4 IC Vendor’s Cryptography Library Security Guideline

If the MIFARE product makes use of a certified Cryptographic Library provided by the IC vendor then the reference including version number of the guidance documentation for this should be provided here. If no use is made of a previously certified Cryptographic Library then please write Not Applicable, or N/A. This will have to be taken into account of in the planning of the test campaign for the product.

4.4.5 Evidence of a Cryptographic Library Security Certificate

Please enter the certificate number of the Cryptographic library detailed in section 2.4.4. If there is no library used or no certificate available then please write Not Applicable or N/A.

4.5 Platform Documentation and Information

Information should be provided in this section if a platform has been used. Otherwise leave this section blank.

4.5.1 Point of contact

Please enter the main contact for information on the platform. This should be someone with access to all relevant security certification information for the platform.

4.5.2 Platform Datasheet

Please provide the datasheet reference including version number for the platform.

4.5.3 Platform security Guidelines

Please provide the reference including version number for the guidance documentation which is required for the underlying security certification of the platform.

4.6 Security Lab and Certification Authority Selection

NXP will provide a list of labs that may be used to perform the product evaluation and another list of labs who may act as a Certification Authority. As most EMVCo and CC certified labs are acceptable for use in either role there will be a considerable overlap in the two lists. Please indicate the selection you wish to make for the evaluation lab and for the certification authority.

4.6.1 Security Lab selected

Please enter the name of the Security lab you wish to use for the product evaluation.

4.6.2 Certification Authority selected

Please enter the name of the lab you wish to use as a Certification Authority.