Certification to ensure conformity to or interoperability with MIFARE products

Conformity to and interoperability with MIFARE products is vital to the success of products, manufactured by or under license of NXP, and to that of implementations, designed to work with MIFARE products. Especially with an ever-increasing number of companies that manufacture licensed products or implementations.

Of equal importance to the success of those solutions and to MIFARE is that this conformity to and interoperability with MIFARE products is established independently. Independent test houses and certification institutes offer worldwide certification for those licensed products and implementations, that meet the requirements for MIFARE.

Independent certification ensures (tendering) parties that they can rely on the fact that certified card products from any supplier will work correctly with any certified terminal/reader. Certified products demonstrate commitment to quality, interoperability and reliability and establish trust with customers.

Certification is done from two angles:

1. Functional Certification
2. Security Certification

It is recommended that applicants first gain Functional Certification of their products before proceeding with Security Certification.

Functional Certification

Functional Certification ensures that the implementation of the respective MIFARE product conforms with all requirements and is primarily used to guarantee that the card, user media or reader products from a supplier will work correctly with any certified terminal or reader. Certified products fulfill the functional requirements in quality, reliability and interoperability for smart and secure MIFARE contactless ICs.

Functional certification can consist of 2 levels, depending on the product.

Functional Certification Level 1

Level 1 ensures that the licensed product implementation shows the correct behavior according to the specification of the respective MIFARE product. This includes NXP's MIFARE ICs as well as implementations from licensees.

Level 1 offers functional certification of licensed MIFARE product implementations. The Level 1 certificate allows vendors, such as card manufacturers, to identify functionally correct products for their solutions. The test house's thorough understanding of the technical requirements, in-depth knowledge about smart cards and mobile devices, combined with a clear certification process will certify the quality of the licensed MIFARE product implementations while maintaining a fast time to market.

Functional Certification Level 2

Level 2 concerns the testing and certification of the proper MIFARE product functionality on the RFID (air) interface (ISO/IEC 14443A part 3). Wave shapes and timing conditions are measured according to the respective ISO specification and with

extended requirements for products. This concerns smart card, user media and inlay products as well as reader/writer terminal products.

The following independent test houses provide Functional Certification services:

UL (Functional Certification – Level 1)

UL is a world leader in advancing safety. UL Transaction Security offers advisory services, test and certification services, security evaluation services, training, and test tools.

Arsenal Testhouse(Functional Certification – Level 2)

Arsenal Testhouse is experienced in certifying contactless transmission via an RF interface. Its experts provide support from the development phase to the manufacture stage, as well as testing and consulting services.

LSI-TEC (Functional Certification – Level 2)

LSI-TEC certifies the interoperability of cards containing MIFARE IC products and qualifies inlays according to particular test specifications. LSI-TEC validates the interoperability of MIFARE IC-based cards to ensure the certified card is able to establish reliable communication through an ISO/IEC 14443 compliant RF interface with reader terminals from different manufacturers.

Security Certification

Security Certification ensures the correct implementation of security-related features in MIFARE ICs, required to provide a secure environment for system providers and end-users.

This certification can be achieved in three ways:

Common Criteria Evaluation to EAL4+ (EAL4 augmented by ALC_DVS.2 and AVA_VAN.5) level (see commoncriteriaportal.org)
Evaluation according to the Security Certification scheme V2.0 for MIFARE products which is based on international standards used for banking grade security. This scheme is conducted by independent test houses and governed by NXP
Evaluation according to the Security Certification scheme V3.0 for MIFARE products which is based on Common Criteria with highly optimized evidence requirements. The products are covered in Protection Profiles. This scheme is conducted by a private independent Certification Authority and independent test houses

Common Criteria Evaluation

The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408 and ISO/IEC 18045) for computer security certification. Security certification can be performed within any of the SOG-IS participating schemes qualified for EAL1-7 for “Smartcards and similar devices” (see www.sogisportal.eu for more details).

Security Certification scheme V2.0 for MIFARE products

This Security Certification scheme for MIFARE products requires resistance against attackers with attack potential “high” according to the JIL Hardware Attack Subgroup (JHAS) document “Application of Attack Potential to Smartcards”. This is the same level of attack resistance as used for a Common Criteria evaluation. The evaluation process under the Security Certification Scheme is optimized and tailored to MIFARE product-based applications. Hence being able to reduce generic documentation efforts with a focus on the implementation security of MIFARE products. This, in turn, results in less time spent for the evaluation and lower costs.

Have a look at already successfully issued Security Certificates.

Security Certification scheme V3.0 for MIFARE products

The Security Certification scheme V3.0 for MIFARE products uses the solid base of Common Criteria (CC) and is driven by the independent certification authority TrustCB, who acts as a single entity for scheme questions and oversees all related MIFARE product evaluations.

The benefits for licensees are the option to re-use the existing CC documentation as well as other solid evidence for MIFARE product evaluations, in a way that is optimized for a well plannable time to market time to certificate.

The MIFARE product certifications conducted under this Security Certification scheme are compliant with EAL4 and augmented by ALC_DVS.2 and AVA_VAN.5.

Please note, that for ease of transition, already running and registered products under the Security Certification scheme V2.0 can continue including the respective renewal processes, with the existing certifying labs or TrustCB acting as certifying lab. Smooth transition from V2.0 to V3.0 is also available.

Advantages of the Security Certification scheme for MIFARE products

Less overhead effort on manufacturer/evaluator side
Reduced time to market
Delivering same attach resistance level of security as for Common Criteria
Less expensive compared to the Common Criteria certification process
Avoidance of bottlenecks at labs, CA capacities or internal resources for work on CC

How to Apply for Security Certification

Security Certification scheme V2.0 for MIFARE products

The Security Certification scheme V2.0 for MIFARE products is available for new product evaluations until the end of 2018. Applications for new product evaluations under this process must be received by December 31st, 2018, and evaluations must be finalized by September 30th, 2019.

Renewals of existing security certificates can be conducted under the Security Certification scheme V2.0 setup until their respective end of life.

You can download the presentation about the Security Certification scheme for MIFARE products for more information.

1. To make inquiries please fill in the Application Form and send it to mifarecertification@nxp.com.
2. To start a renewal for an existing certificate please also fill in the Application form and include a corresponding remark when you send the same to mifarecertification@nxp.com.
3. The possible start date for a renewal security evaluation is six months before the expiration date of the existing Approval letter. The extended life cycle will be linked to the previous expiration date.
4. After the submission, you will receive an extended PRN Number which is 1:1 related to the initial one, i.e. PRN_yyyy_xxx_Rxx (R=renewal). In the same manner we will proceed when we issue the Approval Number, i.e. ARN_yyy_xxx_Rxx (R=Renewal).

The following independent and globally reputed laboratories meet the requirements of the Security Certification scheme for MIFARE products:

Download the labs list

Security Certification scheme V3.0 for MIFARE products

The Security Certification scheme V3.0 for MIFARE products is available for new product evaluations now. You can download the scheme materials and the scheme description here.

1. To make inquiries please fill in the Application Form.
2. The application form registers an IT security assessment under the provisions of the MIFARE scheme operated by TrustCB.
3. The application form needs to be countersigned by the Developer and the evaluator.

4. After submission of the Application form, together with the Security Target and the Evaluation Work Plan (EWP) to mifare@trustcb.com you will receive a dedicated Certification ID together with a Certification Agreement.
5. For maintenance or re-certification:
   The evaluation tasks may be reduced by reusing previous evaluation results >> Reference of original certificate and latest issue date is required.

A scheme overview of the Security Certification Scheme V3.0 for MIFARE is also available here.

For questions regarding the Security Certification process for MIFARE products please contact:

mifare@trustcb.com
mifarecertification@nxp.com