TRUST AND VERIFY

TrustCB Scheme Procedures for MIFARE

Version 2.2

Contents

1 MIFARE Scheme

This document an annex to TrustCB Shared Scheme Procedures version 2.0 [TrustCB_SP] detailing the pertinent details for the MIFARE scheme.

1.1 Introducing the MIFARE scheme

NXP Semiconductors has chosen TrustCB as the centralised Certification Body for the MIFARE Security Certification scheme.

The primary source of information and the TrustCB scheme procedures and documents can be found at https://trustcb.com/global-ticketing/mifare. Supplementary information can be found out https://mifare.net/en/about-mifare/certification

The procedures specific to the operation of the MIFARE scheme are detailed in [MIFARE].

1.2 MIFARE Contact details

Scheme contact address at TrustCB is mifare@trustcb.com.

1.3 MIFARE TOE-type overview

This scheme applies to a TOE implementing MIFARE functionality.

1.4 MIFARE Process

Prior to the submission phase, the developer has contracted a licensed evaluation lab and together with that lab has filled in the application form. A signed copy of the application form, together with a draft Security Target, must be sent by email to mifare@trustcb.com. TrustCB will respond with a quotation for certification for acceptance by the certification sponsor. Upon receipt of acceptance of the quotation, TrustCB will issue an invoice for the payment of the certification fee.

The evaluation phase can commence once that quotation has been accepted and the certification fee paid.

When submitting the application form, the Sponsor may include application for extra certificates for additional variants of the TOE. This is possible only where the additional variants of the TOE will have changes that have a minor impact on the original TOE. The application for such 'maintenance' of the TOE can only be made in combination with an application for a standard TOE certification. The reason for this is that the baseline certification on which the maintenance is to be based requires certain additional reuse-limit details to be reported in the evaluation phase.

1.4.1 Evaluation Phase

As defined in [MIFARE], there are two stages to the Evaluation phase in the MIFARE scheme:

- Vulnerability analysis and test plan. This phase is detailed in [MIFARE] Chapter 3, section "Evaluation phase (vulnerability analysis and test plan)".
- Test results. This phase is detailed in [MIFARE] Chapter 3, section "Evaluation phase (test results)"

If a notice for maintenance was included in the application, the ETR must contain a notice of the reuse limit for the reported results. The reuse limit must indicate the earliest date of expiry for:

- Site audit results: These can be reused for 2.5 years from the date of the site audit.

- Test results: These can be reused for 12 months from the date of the test execution.
- Referenced certificates (e.g. function test results from other certification schemes): By default, these can be reused for 12 months from the date of the certificate. However, in some instances (such as functional testing where the results do no degrade over time) the certificate can be reused until there is a change to the certification scheme the certificate was issued under.

Together these dates will provide the details of the limit within which the maintenance activity can take place. If any expiry date is exceeded then it is not possible to perform a maintenance activity.

In addition, if a certificate is required when non-TSF portions of the TOE are updated, the TOE identifier in the Security Target needs to identify those components that are non-TSF (e.g. a non-TSF applet).

In the maintenance activity the evaluator must first confirm the activity is within the limits of reuse. The evaluator must assess the impact of the changes described by the developer and to re-confirm the verdict for each assurance activity, performing additional source code analysis and testing as necessary. The evaluator must ensure the changes only affect the non-TSF portions of the TOE identified in the Security Target of the baseline TOE.

1.4.2 Certification Phase

As defined in [MIFARE], the certificate validity period for MIFARE certificates is three (3) years from the ETR issue date. This period can be extended by another 1.5 years (18 months), if required, is accordance with the rules defined in [TrustCB_SP] "*Certificate validity*".

If the application included notice of an extra certificate for a minor variant, the certification can be re-issued following a successful maintenance activity by the evaluator, which reports that the maintenance in within the reuse limits, all assurance activity verdicts are still 'Pass' and the changes are to non-TSF portions of the (baseline) TOE. The re-issued certificate will be identified through an increase in the certificate iteration identifier and the issuance date (i.e. a certificate with certificate iteration identifier '-01' will be reissued with '-02', and the date entry on the certificate will list the original certificate issuance date and the 2nd issuance date. The certificate expiry date will stay the same. The re-issued certificate will be posted on the scheme website. The original certificate will also be retained on the website.

1.5 Reference Materials

Unless otherwise stated, the latest published version applies.

Table 1 MIFARE Documents

Title	Source	Reference
MIFARE Scheme	1	[MIFARE]
TrustCB Application Form - MIFARE	1	[MIFARE-AF]
TrustCB Shared Procedures	1	[TrustCB_SP]

Key:

1 = https://trustcb.com/global-ticketing/mifare/

Annex A Revision History

Version	Date	Description of change	Editor
2.1	2020-05-11	Certificate rules: for extra certificates and also where non-TSF portions of the TOE are updated	D Cater
2.2	2020-07-07	Requirements on reuse limit for the reported results	D Cater