TRUST AND VERIFY

TrustCB Scheme Procedures for MDSCert

Version 1.0

Contents

1 MDSCert

This document, as an annex to TrustCB Shared Scheme Procedures [TrustCB_SP], details the scheme specific details for the MDSCert scheme.

1.1 Introducing the TrustCB MDSCert scheme

GSMA has designed and specified the requirements for a "Mobile Device Security Certification (MDSCert)" scheme. In such MDSCert schemes "mobile devices are evaluated against the GSMA MDSCert Security Requirements for the security evaluation of mobile devices, which are based on the ETSI Consumer Mobile Device Protection Profile ([ETSI TS 103 732] series)". As described in [FS.53], [FS.54], [FS.55] and [FS.56], this scheme design is intended "to be implemented by any scheme owner", in this case TrustCB as scheme owner and operator.

Thus the MDSCert scheme checks conformance of consumer devices against [ETSI 103 7032].

This document, together with the TrustCB Shared Scheme Procedures [TrustCB_SP], defined the TrustCB MDSCert scheme, "MDSCert" for short.

The primary source of information and the TrustCB scheme procedures and documents can be found at https://trustcb.com/gsma/mdscert/.

1.2 MDSCert Contact details

Scheme contact address at TrustCB is: mdscert@trustcb.com.

1.3 TOE-type overview

The TOE-type is a consumer device complying to [ETSI TS 103 732], usually a "handheld device produced by a Mobile Device Manufacturer used to make and receive phone calls and mobile messages, support voicemail and connect to the Internet over Wi-Fi or a cellular network" or derived device such as tablet, chromebook, and TV running these mobile OSes.

The security functionality required from these devices is expressed in the [ETSI TS 103 732] Protection Profile.

Summarized as per [FS.53]:

"The security baseline, and the product evaluations to assess compliance with it, address:

- Hardware.
- Firmware.
- Operating system.
- Pre-loaded software.
- In-life software updates.

The security surfaces include:

- Physical interfaces
- Logical interfaces

The following are excluded as they are typically addressed by other existing dedicated schemes:

- 3GPP Mobile Radio interfaces (e.g. 5G RAN).
- UICC and/or eUICC" (e.g. GSMA eSA)."

"The certification of a Mobile Device applies to the factory specification product. The certification does not apply to:

- Third-party software or applications added (intentionally or unintentionally) post-production, including additions by users and/or supply chain participants (e.g. retail stores, mobile operators, etc.).
- Modifications made to the originally provided software (intentionally or unintentionally), post-production.
- Physical modifications made to the product, post-production.
- Repaired products where such repairs are not carried out using Mobile Device Manufacturer certified parts and by a Mobile Device Manufacturer approved repair facility.

The certificate does not apply to user behaviour which has the potential to compromise mobile device security, such as:

- Providing passwords or other security credentials to third parties (intentionally or unintentionally).
- Failing to install in a timely manner or blocking installation of security-critical updates.
- Failing to keep third-party applications up to date.
- Connecting insecure peripherals (e.g. Bluetooth headphones).
- Intentionally or unintentionally granting insecure permissions to applications which were blocked by default in the certified configuration.
- Using the product over insecure / high risk networks (e.g. airport Wi-Fi)."

1.4 Security Assurance Levels

MDSCert has three Security Assurance Levels:

1. Security Assurance Level 1: Verified Self-assessment

   At this level, a verification by the lab on the developer's self-assessment, no verification by the certification body.

2. Security Assurance Level 2: Functional Test + Document Review

   At this level onwards, on-device functional testing is performed (and devices for testing need to be provided to the lab). The certification body verifies following of pre-checked test procedures by the lab.

3. Security Assurance Level 3: Level 2 + Penetration test.

   At this level, on-device penetration testing is performed at AVA_VAN.2 (Basic Attack Potential) level. The certification body verifies the vulnerability analysis and penetration testing done on a per project basis.

2 MDSCert Process

The MDSCert process follows the TrustCB Shared Scheme Procedures.

2.1 Application phase

For clarity and to ensure that the certificate is meaningful, the remaining support period for the mobile device must be at least two (2) years after the successful completion of the evaluation activities and issuing of the certificate.

2.1.1 Application phase for Security Assurance Level 1

At Security Assurance Level 1, the application, developer evidences and the evaluator's pass verdict are delivered together.

For optimization, the application phase for level 1 is combined with the evaluation phase.
To avoid delays on financing, invoicing should run via the lab where possible.

2.1.2 Application phase for Security Assurance Level 2 and 3

Prior to the submission phase, the developer shall have contracted a licensed evaluation lab and, together with that lab, have filled in the application form. A signed copy of the application form, together with the questionnaire (forming the Security Target for the TOE), must be sent by email to mdscert-application@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.

2.2 Evaluation Phase

The default process for evaluations under the MDSCert scheme as Security Assurance Level 1 and 2 is a one stage Evaluation Phase, for Security Assurance Level 3 is for a two stage Evaluation Phase as per TrustCB Shared Scheme procedures [TrustCB_SP].

In the case of a Security Assurance Level 3 evaluations, the two stages to the Evaluation Phase are:

- Vulnerability analysis and functional and vulnerability test plan (EM1+EM2 in [TrustCB_SP]), at AVA_VAN.2 level.

- Test results (EM3 in [TrustCB_SP]).

Note that [FS.55] contains useful guidance on the testing and analysis.

In all cases the result of the successful completion of these the evaluation phase is the issuance of a full pass ETR by the licensed lab to TrustCB.

2.3 Certification Phase

Based on the pass ETR, TrustCB will make a certification decision as per TrustCB Shared Scheme Procedure [TrustCB_SP].

The certificate validity period for MDSCert certificates is two (2) years from the ETR issue date. Because of the "MDSCert Scheme Certificate Validity Period" [FS.53], This period can be extended by another two (2) years, if required, is accordance with the rules defined in [TrustCB_SP] "Certificate maintenance".

All certificates, including those no longer valid and archived, are published on the scheme website.

All parties are warned that only valid and published certificates may be used to claim a Mobile Device is compliant or certified in accordance to MDSCert security requirements. Invalid claims of certification should lead to revocation to one or more of the manufacturers certificate (always public), and can lead to rejection of future applications to the MDSCert for the offending developer.

2.4 Scheme optimizations

2.4.1 Re-use of reference mobile device certificates

A certificate for Reference Mobile Device (RMD) can be "re-used" (MDSCert term) following the "Maintenance of the certified TOE that does not impact the certified security claim" in TrustCB Shared Procedures [TrustCB_SP], by showing compliance to the same security claims for a similar new mobile device, if the similarity can be shown convincingly.

The developer shall provide:

- A list of differences between the RMD and the new Mobile Device, focusing on the security-relevant components used for the RMD Certification.
- An equivalence analysis of the similarity between the device models.
- If the Mobile Device is being evaluated separately from the RMD, an updated MDSCert Questionnaire for the new device (new device information and any changes as needed in the questionnaire based on the new device).

The evaluator shall verify that the new mobile device is similar, including but not limited to verifying that:

- The main OS version is the same.
- SoC is the same - a later iteration of the SoC, which may have performance benefits and may be acceptable, subject to MSCB approval.
- Composition components are the same. (Note that any replaced/changed components from the RMD disallow certification by similarity for the new Mobile Device.)

For more detailed suggestions, see section "Multiple Mobile Devices and Similarity" of [FS.53].

2.4.2 Re-use of component certificates

CCRA and EUCC Common Criteria or TrustCB SESIP component certificates for underlying components such as the hardware platform may be re-used in a MDSCert evaluation and certification at the acceptance of TrustCB.

The evaluator must describe and verify how the scope and level of the component certificate contributes to the scope and role of the component security functionality in the MDSCert functional and assurance requirements. The sponsor and evaluator are advised to indicate these plans in the application to reduce project risks (of the certifier not agreeing with the composition).

MDSCert follows the suggestions of [FS.55] and the following assurance levels should be sufficient:

"For Security Assurance Level 1:

- SESIP1.
- CC EAL1.

- NIST CMVP Level 1.
- ISO/IEC 19790 Level 1

For Security Assurance Level 2 & 3:

- SESIP2.
- CC EAL2.
- NIST CMVP Level 3.
- ISO/IEC 19790 Level 3"

The underlying component certificate should at most 1.5 years old at the time of issuance of the Mobile Device ETR, and must have at least one year remaining validity.

For all Security Assurance Levels, a valid NIST CAVP certificate for that component version can be used for the functional compliance of the cryptographic implementation (can be more older than 1.5 years).

2.5 Certification Marks and Logos

The TrustCB issued certificate for a compliant product includes a TrustCB owned CC Certification Mark.

3 Lab licensing requirements

As described in [FS.34], labs are required to:

1. Have and maintain a valid accreditation for conformance assessment against [ETSI TS 103 732] in the form of:
   a) A valid ILAC ISO/IEC 17025 accreditation including the Common Criteria scope.
   b) Recognition as authorized ITSEF under CCRA Recognised Scheme.
2. Show and maintain qualifications in performing security evaluations considering state-of-the-art attackers equivalent to AVA_VAN.2 as defined in Common Criteria, for this TOE type.
3. Agree to terms and conditions for participation in the scheme.

All these aspects are covered by the TrustCB lab yearly licensing process.

4 MDSCert Reference Materials

The documents listed in Table 1 are specific to the MDSCert scheme.

Table 1 MDSCert Documents

Title	Source	Reference
"Consumer Mobile Device Protection Profile and related documents", ETSI TS 103 732 defined by ETSI: ETSI TS 103 932-1 - V1.1.2 - CYBER; Consumer Mobile Devices Base PP-Configuration; Part 1: CMD and Biometric Verification ETSI TS 103 732-1 - V2.1.2 - CYBER; Consumer Mobile Device; Part 1: Base Protection Profile ETSI TS 103 732-2 - V1.1.2 - CYBER; Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module	ETSI	[ETSI TS 103 732]
FS.53 CR1001 (New PRD): Mobile Device Security Certification Scheme - Overview	https://gsma.org	[FS.53]
FS.54 CR1001 (New PRD): Mobile Device Security Certification Scheme - Security Test Laboratory Accreditation	https://gsma.org	[FS.54]
FS.55 CR1001 (New PRD): Mobile Device Security Certification Scheme – Evaluation Methodology	https://gsma.org	[FS.55]
FS.56 Mobile Device Security Certification Scheme – GSMA Security Requirements	https://gsma.org	[FS.56]
TrustCB Shared Scheme procedures, latest version	https://trustcb.com	[TrustCB_SP]

Note: Refer to the Application Form, section "A.1 Scheme references", for all reference document versions defining the scheme at the time of application.

Annex A Revision History

Version	Date	Description of change	Editor
1.0 draft	2024-11-02	Initial version	W. Slegers
1.0	2025-02-07	First public version	W. Slegers