Mobile Device Security Certification Scheme - Security Test Laboratory Accreditation

Version 1.0

18 September 2024

Security Classification: Non-Confidential

Copyright Notice

Disclaimer

Compliance Notice

The information contain herein is in full compliance with the GSMA Antitrust Compliance Policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1 Introduction

This document forms part of the documentation of the Mobile Device Security Certification Scheme (MDSCert). An overview of the scheme is available in GSMA PRD FS.53 [5] – Mobile Device Security Certification Scheme - Overview.This document defines the requirements for MDSCert Security Test Laboratories and sets the standard against which accreditation is to be assessed and awarded. The document provides an overview of the MDSCert Security Test Laboratory accreditation process.

1.1 Scope

The scope of this document is the MDSCert Security Test Laboratory Accreditation requirements and process.

The accreditation requirements defined in this document ensure that accredited MDSCert Security Test Laboratories have the capabilities to perform evaluation of mobile devices under the MDSCert scheme.

1.2 Document Maintenance

The MDSCert scheme documentation was originally created and developed by GSMA's Mobile Device Security Certification Working Party that was comprised of representatives from Mobile Network Operators, Mobile Device Manufacturers, operating system developers and test laboratories. Ongoing responsibility for maintenance and development of the MDSCert scheme documents rests with GSMA's Device Security Group, which will facilitate periodic reviews involving all relevant stakeholders.

1.3 Definitions

Term[1]	Description
Certification	The granting of a certificate for a Mobile Device that has been subjected to a Mobile Device Evaluation
Consumer Mobile Device Protection Profile	Specification written by ETSI (ETSI TS 103 732 series [2]) containing the security requirements for a security evaluation of consumer mobile devices.
Evaluation Testing Report	The report created by the MDSCert Security Test Laboratory containing the analysis and results of the Product Evaluation that is presented to the MDSCert Certification Body.
Evaluator	Person acting on behalf of an MDSCert Security Test Laboratory.
GSMAMDSCert Security Requirements	A set of security requirements defined by GSMA, that shall be tested and verified, based on the requirements defined in the Consumer Mobile Device Protection Profile (ETSI TS 103 732 series [2]).
MDSCert Scheme	The certification body executes the procedures and reviews and validates the work performed by MSTLs to ensure consistency and quality of the Mobile

[1] Unless otherwise defined, all capitalised terms shall have the same meaning as in GSMA FS.53 [5].

Term[1]	Description
Certification Body	Device Evaluations. The Certification Body is also tasked with performing surveillance on evaluated products.
ISO/IEC 17025 Accreditation Body	An ILAC member that is recognised as having competence to carry out ISO/IEC 17025 test laboratory audits.
MDSCert Security Test Laboratory	A test laboratory that is ISO/IEC 17025 accredited in the context of MDSCert and that conducts MDSCert Mobile Device Evaluations. It can be owned by any entity.
Mobile Device	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.
Mobile Device Evaluation	An assessment, carried out by a MDSCert Security Test Laboratory, of mobile device compliance against the ETSI Consumer Mobile Device Protection Profile (ETSI TS 103 732 series [2]) and GSMA MDSCert Security Requirements contained in the MDSCert scheme documents.
Mobile Device Manufacturer	Organisation that develops, maintains and supplies mobile devices that support cellular technologies defined by 3GPP.
Protection Profile	Specification containing the security requirements for a security evaluation.
Scheme Owner	The organisation tasked with the overall implementation, governance, management and further development of MDSCert.
Test Laboratory Accreditation	The process by which a security test laboratory is assessed by a qualified ISO/IEC 17025 Accreditation Body to assess and accredit its level of competence.

1.4 Abbreviations

Term	Description
3GPP	3rd Generation Partnership Project
CB	Certification Body
ETSI	European Telecommunications Standards Institute
GSMA	GSM Association
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
ILAC	International Laboratory Accreditation Cooperation
ISO	International Standards Organisation
MDSCert	Mobile Device Security Certification Scheme
MSTL	MDSCert Security Test Laboratory

1.5 References

Ref	Doc Number	Title
[1]	RFC 2119	“Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt

Ref	Doc Number	Title
[2]	ETSI TS 103 732 et al	"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
[3]	ISO/IEC 17025	"General requirements for the competence of testing and calibration laboratories", 2005
[4]	ISO/IEC 17011	"Conformity assessment -- General requirements for accreditation bodies accrediting conformity assessment bodies", 2004
[5]	GSMA PRD FS.53	MDSCert Scheme Overview.

1.6 Conventions

"The key words "must", "must not", "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this document are to be interpreted as described in RFC2119 [1].

2 Selection of ISO/IEC 17025 for MDSCert Security Test Laboratory Accreditation

ISO/IEC 17025 [3] has been selected as the standard to be achieved by security test laboratories under MDSCert. This section outlines the motivation for selecting ISO/IEC 17025.

ISO/IEC 17025 is an international standard for accrediting test laboratories. It is general and can be used to accredit any test laboratory, irrespective of the product under test.

ISO/IEC 17025 is well established and there is an existing infrastructure of accreditation bodies.

The International Laboratory Accreditation Cooperation (ILAC) makes it possible for accreditation bodies to mutually recognise accreditation by, and from, other accreditation bodies. The accreditation bodies participating in ILAC must conform to ISO/IEC 17011 [4] to demonstrate that they are capable of accrediting test laboratories.

ISO/IEC 17025 is the single global standard used for test laboratory accreditation.

The goal of ISO/IEC 17025 accreditation is to ensure worldwide comparable accuracy and correctness of output created by a test laboratory. This ensures that all stakeholders can trust evaluation reports created by an ISO/IEC 17025 accredited test laboratory.

ISO/IEC 17025 provides for the independence and impartiality of test laboratories. Any test laboratory that is ISO/IEC 17025 accredited is eligible to be recognised as a MDSCert Security Test Laboratory under the scheme.

3 Security Objectives

MSTLs are responsible for ensuring their assets are protected from the risks to which they are exposed. It is this protection that provides assurance to the Mobile Device Manufacturers and other industry stakeholders. A range of security objectives must be addressed but higher levels of assurance are needed depending on the asset classification.

The desire is to ensure that Accreditation of an MSTL under the MDSCert Scheme ensures that MSTLs are set up and maintained that are capable of performing meaningful, comprehensible, repeatable, and complete tests of Mobile Devices. MSTLs must maintain the existence and integrity of their assets and must ensure they reach and maintain the standard described in this document.

4 MDSCert Security Test Laboratory Assets

The main assets of a MSTL that need to be protected guaranteed and held are:

- Competence of the laboratory personnel
- Understanding of threat landscape and threat actor techniques, tactics, and procedures
- Working processes and guidelines for the laboratory
- Equipment and tools available to, and used by, the laboratory.

5 MDSCert Security Test Laboratory Threats

Threats related to the security of MSTL assets and to which they are exposed include:

- The laboratory personnel are not sufficiently competent
- The laboratory lacks understanding of threat landscape and threat actor techniques, tactics, and procedures
- The laboratory lacks suitable working procedures and guidelines
- The laboratory lacks suitable equipment and tools.

6 MDSCert Security Test Laboratory Requirements

In order to have sufficient confidence in the competence and capabilities of the MSTL, certain requirements must be met. The overriding requirement is to achieve ISO/IEC 17025 [3] accreditation, which encompasses a range of requirements that must be satisfied.

The MSTL must be specifically ISO/IEC 17025 accredited to perform tests as defined by the MDSCert Scheme.

To be recognised as a competent test laboratory, MSTLs must have and demonstrate the requisite expertise, capabilities, equipment, procedures, and environment. The MDSCert Scheme has defined guidelines that can be used by the Scheme Owner for test laboratories and ILAC member accreditation bodies on what is expected of candidate MSTLs to demonstrate their competency and have MDSCert included in the scope of their ISO/IEC 17025 accreditation. Full details are available in Annex A below.

MDSCert Scheme requires that the defined period for which reports and relevant records, as defined in section 8.4 in ISO/IEC 17025, must be retained is the lifetime of the Mobile Device.

7 MDSCert Security Test Laboratory Accreditation Process

The MDSCert Security Test Laboratory accreditation process exists to formally recognise that a security test laboratory is impartial and competent to evaluate a Mobile Device against the GSMA MDSCert Security Requirements based on the ETSI Consumer Mobile Device Protection Profile (ETSI TS 103 732 series [2]), and to produce an Evaluation Report by the MDSCert Scheme.

The MDSCert CB(s), under guidance from the Scheme Owner, will manage the accreditation process for candidate test laboratories to become an MSTL. The candidate security test laboratory shall apply to the MDSCert CB(s), following its ISO/IEC accreditation, and provide evidence of meeting the accreditation requirements. The MDSCert CB will then review the provided evidence to determine whether accreditation is granted within the scheme.

There are two methods for a security test laboratory to become a MSTL. GSMA has established a baseline for the Scheme Owner to use for all methods of an ISO/IEC 17025 accreditation, which shall be complete before consideration of a candidate test laboratory becoming an MSTL.

7.1 Step 1 - Common Accreditation Requirements

The first step to achieve accreditation, and be recognised as a test laboratory capable of evaluating product compliance against security requirements, is for a security test laboratory to contact a recognised ILAC member ISO/IEC 17025 accreditation body with a request to be ISO/IEC 17025 audited and accredited. The ISO/IEC 17025 accreditation body will follow the processes applicable to the ISO/IEC 17025 accreditation standard to assess the competence of the security test laboratory.

In addition to the requirements defined in the ISO/IEC 17025 standard, additional security requirements that need to be fulfilled as part of the MDSCert Security Test Laboratory Accreditation process may be adopted. The requirements beyond the ISO/IEC 17025 standard may be fulfilled in multiple ways.

7.2 Step 2 - ISO/IEC 17025 with MDSCert Competency

The ISO/IEC 17025 accreditation body shall be provided with a copy of the current version of this document including the MDSCert Security Test Laboratory Competency Requirements contained in Annex A below, to ensure it understands what competency requirements are applicable at the time the accreditation is sought.

The Scheme Owner fully recognises the competency of ILAC member accreditation bodies to assess and accredit security test laboratories. Therefore, all security test laboratories that are deemed by an ILAC member to have satisfied the ISO/IEC 17025 and MDSCert competency requirements, and that have been ISO/IEC 17025 accredited, will be considered to have achieved MDSCert Security Test Laboratory accreditation.

After ISO/IEC 17025 accreditation has been achieved the successful security test laboratory will inform the Scheme Owner and provide a copy of its ISO/IEC 17025 certificate, referencing MDSCert. The laboratory's details (including validity dates) will be recorded and published on the Scheme Owner's MDSCert Website. It is the responsibility of the MDSCert Security Test Laboratory to keep its ISO/IEC 17025 accreditation current. Failure to do so will cause its recognition of its competency to conduct Mobile Device Evaluations to lapse and become invalid.

7.3 Step 3 - Provisional Accreditation with Trial Evaluation

In addition to the requirements defined in the ISO/IEC 17025 [3] standard, the security test laboratory shall prove competency in the MDSCert Security Test Laboratory Competency Requirements contained in Annex A below directly to the MDSCert CB. The security test laboratory shall provide evidence to show competency, regardless of the ISO/IEC accreditation.

Upon acceptance of the evidence of competency, the MDSCert CB shall issue a provisional accreditation to the security test laboratory. This accreditation allows the security test laboratory to perform an initial evaluation under scrutiny from the MDSCert CB.

The MDSCert CB will require regular meetings and updates with the provisional MSTL to ensure the successful completion of the evaluation. Upon successful completion of the evaluation, the MDSCert CB can issue a full accreditation. This accreditation would not be for a period longer than the remaining validity period of the ISO/IEC 17025 accreditation.

Upon renewal of the ISO/IEC 17025 accreditation, the MDSCert CB will review and determine whether to reauthorize the MDSCert accreditation (for the same time-period).

Annex A MDSCert Security Test Laboratory Competency Requirements

A.1 Introduction

One of the requirements defined under the Mobile Device Security Certification Scheme (MDSCert) is that MSTLs are accredited to ISO/IEC 17025 [3]. As part of that accreditation, the MSTL must demonstrate its competencies to undertake MDSCert Mobile Device Evaluations against the security requirements defined by the MDSCert Scheme.

This document describes the experience and skills that Evaluators in the MSTL must have to execute their role effectively in order to meet the competency requirements of MDSCert.

A.2 Purpose

This annex is primarily intended to guide organisations that

- Apply to be recognised MSTLs that operate under the MDSCert rules or
- Act as ISO/IEC 17025 Accreditation Bodies for MSTLs.

A.3 Overview

The process for awarding MDSCert Security Test Laboratory Accreditation is designed to ensure that the candidate test laboratory has sufficiently demonstrated that it is technically competent in the specific field of ICT security evaluation under MDSCert.

The MDSCert accreditation process includes the need for the test laboratory to demonstrate that it, and specifically the Evaluators assigned by the test laboratory, have the ability to execute test cases relevant to the MDSCert Scheme.

A.4 Evaluator/Evaluation Team Competency

The requirements provided below act as supplementary competency requirements to the requirements contained in ISO/IEC 17025 [3]. They are intended to be helpful to experts collaborating and supporting the ISO/IEC 17025 Accreditation Body (so-called subject matter experts). As such, these guidelines are intended to assist the “subject matter expert” to ensure high quality MDSCert evaluations can be executed by an Evaluator/Evaluation Team.

Evaluators will need to demonstrate relevant knowledge of the tasks they are assigned. The Evaluation Team working within the definition of MDSCert is required to:

- Understand the principles and methods used in MDSCert,
- Understand the relationship between ETSI TS 103 732 series, GSMA MDSCert Security Requirements and other documents used by the MDSCert scheme,
- Demonstrate an understanding of the overall evaluation planning process (i.e. how to interpret the security requirements defined in ETSI TS 103 732 series and GSMA MDSCert Security Requirements, what to look for in terms of compliance, how to plan and execute relevant test cases on Mobile Devices, etc.,
- Be able to analyse the results of the MDSCert testing including vulnerability scans according to the relevant test cases,
- Be able to independently document the evaluation results objectively, precisely, correctly, unambiguously, and at the level of detail required by MDSCert (namely to

create MDSCert Evaluation Testing Reports to the level of detail specified in the ISO/IEC 17025 standard). The MDSCert Evaluation Testing Report must ensure that the level of detail allows for reproducibility of the tests results,

- The Evaluation Team should clearly demonstrate its understanding of the MDSCert evaluation methodology and process including:
    - How MDSCert security requirements are defined in ETSI 103 732 series as well as the GSMA MDSCert Security Requirements,
    - How ETSI 103 732 series and GSMA MDSCert Security Requirements are used to test a specific Mobile Device,
    - What are the inputs to a MDSCert evaluation,
    - What is the meaning of the MDSCert Mobile Device Evaluation to the Mobile Device Manufacturer and other stakeholders.
- The Evaluation Team is expected to be familiar with Mobile Devices and related knowledge, such as security architecture, interfaces, protocols, interaction procedures and messages, typical attack surfaces, attack patterns and vulnerabilities.

In addition to the general competency requirements described in this section, the Evaluation Team shall have sufficient technical competence for the tasks it performs. It is the MDSCert Security Test Laboratory's responsibility to determine the competencies needed within the MDSCert Evaluation Team for each evaluation, to appoint Evaluators accordingly, and, if necessary, to augment the Evaluation Team with internal or external technical experts.

Although not especially specified in MDSCert, it is expected that:

- Evaluators appointed to the Evaluation Team have relevant knowledge, working experience and/or education in order to fulfil the needs to be a MDSCert Security Test Laboratory Evaluator.
- The Evaluation Team has a team leader who is highly experienced to supervise, oversee and monitor the activities of less experienced Evaluators and the additional specialists and technical experts.
- Guidance for identifying relevant knowledge, experience, skills or educational qualifications could be:
- Several years (2-3+) experience working on ICT security testing (security functional testing, penetration testing, ethical hacking, or related fields),
- External security testing qualifications (such as Certified Ethical Hacker, SANS Ethical hacker certification, GIAC certifications).

A.5 Testing Equipment and Tools

An MDSCert Security Test Laboratory should have access to testing equipment and tools for Mobile Device security testing such as fuzz testing tools and scanning tools, which are Commercial-off-the-Shelf (COTS) and Free-Open-Source-Software (FOSS) tools.

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	18 Sep 2024	First version	ISAG	Alex Leadbeater, GSMA

B.2 Licensing of MDSCert Documentation

This GSMA document and its content is:

- the exclusive property of the GSMA; and
- provided “as is“, without any warranties by the GSMA of any kind.

Any official government (or government-appointed) body wishing to use this GSMA document or any of its content:

- for the creation of; or
- as referenced in;

its own documentation regarding the same or a similar subject matter is hereby granted a licence to the copyright in this document.

This grant is subject to and upheld, as long as the above body:

a) informs the GSMA about the use of the GSMA document prior to commencing work on;
b) provides the GSMA with the finalised, i.e. most up-to-date version of; and
c) properly references the GSMA document and any extracts thereof in;

its own documentation.

B.3 Other Information

Type	Description
Document Owner	GSMA FASG DSG
Editor / Company	Alex Leadbeater / GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at mdscert@gsma.com. Your comments or suggestions & questions are always welcome.