Mobile Device Security Certification Scheme - Overview
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

1.1 About the Mobile Device Security Certification Scheme

This document describes the GSMA Mobile Device Security Certification (MDSCert) Scheme. MDSCert aims to provide an industry-wide security assurance framework that increases the transparency of security capabilities of mobile devices, such as smartphones and tablets, with a view to facilitating improvements in security levels across the whole mobile device ecosystem.

The MDSCert Scheme is designed as a complete security certification scheme to be implemented by any Scheme Owner. The Scheme, when implemented, would consist of security evaluations carried out by Scheme Owner authorised MDSCert Security Test Laboratories (MSTL) and overseen by the Scheme Owner appointed Certification Bodies (CB). 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).

The MDSCert Scheme is designed to meet the needs of industry and other stakeholders. The security baseline consists of a set of technical (functional) and non-technical requirements that attest the security capabilities of a mobile device. The security requirements are considered living requirements and will be maintained to reflect the needs of the current security threat landscape.

Under the Scheme, a Mobile Device Manufacturer can apply to have a mobile device product certified against one of three security assurance levels. The compliance level of a product can be self-assessed by the Mobile Device Manufacturer or it can be evaluated by an authorised MSTL against industry defined security requirements. The evaluation results, from the manufacturer or MSTL, are verified by an appointed CB and a Certificate is issued if the product meets the security requirements. The scheme owner issues and publishes the Certificates for eligible products and maintains and updates those Certificates during their validity period, after which they are archived.

The MDSCert Scheme provides assurance that devices meet the scheme's security requirements but does not provide an absolute assertion of perfect security or that previously unknown vulnerabilities or the emergence of new attacks will not impact this assurance over the lifetime of a mobile device.

1.2 Stakeholder Benefits

The MDSCert Scheme is of value to Mobile Device Manufacturers, Mobile Network Operators, mobile device users and a multitude of key opinion formers such as policy makers, technical press, and general press. It is intended to be used alongside other mechanisms to demonstrate that the security posture of mobile devices has been assessed against a comprehensive set of security requirements.

The MDSCert Scheme will help Mobile Device Manufacturers and Mobile Network Operators provide greater visibility to mobile users and other stakeholders on the security capabilities of Mobile Devices. It does so by providing a single reference point where all interested stakeholders can see, in a consistent way, which Mobile Devices have undergone security evaluation and certification against the industry defined security requirements and the results

of those evaluations. The publication of this information increases transparency of how individual Mobile Device models protect users and their data and for how long they will be supported. The globally applicable MDSCert Scheme, in providing objective and consistent security benchmarks, benefits policymakers interested in setting security baselines and promoting better transparency as well as security awareness.

1.3 Document Scope

This document has been produced for stakeholders who want to familiarise themselves with the MDSCert Scheme. It provides an overview of the MDSCert Scheme and defines;

- MDSCert Dispute Resolution Process (MDSCert DRP).
- GSMA FS.53 - MDSCert Scheme Overview.
- GSMA FS.54 - MDSCert Security Test Laboratory Accreditation [5].
- GSMA FS.55 - MDSCert Product Evaluation Methodology [6].

The scheme is based on the use security requirements specified MDSCert security requirements contained in the scheme documents, based on ETSI 103 732 series [2].

This document is relevant to:

- Mobile Device Manufacturers.
- Mobile Network Operators.
- Test laboratories.
- Certification bodies.
- Policy makers.
- Mobile Device Users.
- Media and consumer advice outlets.

An introduction and overview of the MDSCert Scheme is provided in Sections 2 and 3 below. The remainder of this document explains the roles of the actors in the Scheme, functions of the Scheme and Scheme processes. All sections and information in the document are normative unless otherwise indicated.

1.4 Document Maintenance

The MDSCert Scheme documentation was created and developed by GSMA's Device Security Group, comprised of representatives from Mobile Network Operators, Mobile Device Manufacturers, operating system developers and test laboratories. GSMA's Device Security Group will maintain the responsibility for ongoing maintenance and development of the MDSCert Scheme documents and will facilitate periodic reviews involving all relevant stakeholders.

1.5 Definitions

Term	Description
Certification by Similarity	A method for granting the certification of a Mobile Device based on its similarity to a previously tested and certified Mobile Device.
Certifier	Person acting on behalf of a Scheme Owner appointed MDSCert Security Certification Body

Term	Description
Certification	The granting of a certificate for a Mobile Device that has been subjected to a Mobile Device Evaluation
Certification Report	The report created by the MDSCert Scheme Certification Body containing the final determination of evaluation based on the reports provided by the MDSCert Security Test Laboratory.
Compliance Declaration	Documented statement by a Mobile Device Manufacturer of the level of compliance of a Mobile Device with the ETSI Consumer Mobile Device Protection Profile (TS 103 732 series [2]) and the GSMA MDSCert Security Requirements.
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 Scheme Certification Body.
Evaluator	Person acting on behalf of a MDSCert Scheme Test Laboratory
GSMA MDSCert Security Requirements	A set of security requirements defined by GSMA that shall be tested and verified, based on the requirements described in the Consumer Mobile Device Protection Profile (ETSI TS 103 732 series [2]).
ISO/IEC 17025 Accreditation Body	An ILAC member that is recognised as having competence to carry out ISO/IEC 17025 test laboratory audits.
MDSCert Scheme Certification Body	The certification body executes the procedures, reviews and validates the work performed by MSTLs to ensure consistency and quality of the Mobile Device Evaluations. The certification body is also tasked with performing surveillance on evaluated products.
MDSCert Dispute Resolution Process	The process used by the MDSCert DRC to resolve disputes in accordance with Section 15 below.
MDSCert Dispute Resolution Committee	A panel established to adjudicate on disputes pursuant to Section 15 below.
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 by users 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 (TS 103 732 series) and the GSMA MDSCert Security Requirements.

Term	Description
Mobile Device Manufacturer	Organisation that develops, maintains and supplies Mobile Devices that support cellular technologies defined by 3GPP.
Mobile Device Model	A Mobile Device that is part of a Product Family.
Mobile Device Similarity	The state of being the same for a given scope (e.g. hardware platform), or a way in which a Mobile Device component or element (e.g. a functionality) can be considered as equivalent for a given purpose.
Mobile Device Variant	A Mobile Device where software or configuration changes are made that target different markets/carriers, all using a common device.
Product Family	A series of device models which use a common set of components while providing differentiation in market, such as form factor, to meet the security requirements.
Protection Profile	Specification containing the security requirements for a security evaluation.
Questionnaire	Simplified term for the complete set of documents required to show compliance to the MDSCert Scheme security requirements.
Reference Mobile Device	A certified Mobile Device that is used as a basis for comparison to determine whether a second Mobile Device is similar (Certification by Similarity), on the basis of components used in meeting the security requirements.
Scheme Owner	An organisation tasked with the overall implementation, governance and management of MDSCert.
Security Assurance Level	Indicates the degree to which the compliance of a Mobile Device to the MDSCert security requirements has been evaluated.
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.

1.6 Abbreviations

Term	Description
3GPP	3rd Generation Partnership Project
5G	5th Generation
CC	Common Criteria
CCRA	Common Criteria Recognition Agreement
DRC	(MDSCert) Dispute Resolution Committee
ETSI	European Telecommunications Standards Institute
eUICC	Embedded UICC
GSMA	GSM Association
IEC	International Electrotechnical Commission
ILAC	International Laboratory Accreditation Cooperation
ISO	International Standards Organisation.
MDSCert	Mobile Device Security Certification Scheme
MSCB	MDSCert Scheme Certification Body
MSTL	MDSCert Scheme Test Laboratory

Term	Description
OS	Operating System
PP	Protection Profile
RAN	Radio Access Network
RMD	Reference Mobile Device
SESIP	Security Evaluation Standard for IoT Platforms
SoC	System on Chip

1.7 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
[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.54	MDSCert Scheme Test Laboratory Accreditation.
[6]	GSMA PRD FS.55	MDSCert Scheme Product Evaluation Methodology.
[7]	CC 2022 Rel 1	"Common Criteria CC:2022 Release 1". Available at https://www.commoncriteriaportal.org/cc/

1.8 Conventions

"The keywords "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]."

All sections of the document, including annexes, are normative, unless otherwise explicitly stated.

2 Scope of MDSCert

As a security assurance scheme, MDSCert is specifically developed to consider the environment in which the scheme operates. The following aspects are considered:

- Mobile device technology and products.
- Mobile device security lifecycle.
- Visibility of mobile device security assurance levels.
- Market acceptance and participation.

With the increasing utility of, and reliance on, mobile devices and heightened security awareness, MDSCert is designed to meet the needs of a range of stakeholders including:

- Mobile Device users.
- Mobile Device Manufacturers.
- Component suppliers.
- Operating system vendors.
- Mobile Network Operators.
- Official/Governmental information security agencies and regulators.
- Media and consumer advice outlets.

The purpose of the MDSCert Scheme is to provide a framework to certify that a Mobile Device meets the security requirements of a robust industry-specified security baseline defined by GSMA. This is based on ETSI TS 103 732 series [2], as reflected in MDSCert security requirements maintained by GSMA.

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.

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).

3 MDSCert Scheme Overview

The MDSCert Scheme enables participating manufacturers to demonstrate that particular mobile device products have achieved an industry-recognised level of security. Products achieving the necessary security level(s) receive a time-limited certificate to confirm compliance. Certificates may be used to indicate the security credentials of specific mobile device products. Use of the Scheme is voluntary for Mobile Device Manufacturers and they are free to determine which of their products they wish to subject to a security evaluation.

A Scheme Owner can utilise the GSMA MDSCert Scheme documents to implement a certification scheme. In this case, the Scheme Owner operates the MDSCert Scheme and invokes the services of accredited Test Laboratories and Certification Bodies to conduct the product evaluation and certification elements of the scheme, specifically in accordance with the requirements of the GSMA.

The Scheme Owner authorises Test Laboratories that can demonstrate they are qualified, capable and willing to execute GSMA MDSCert product evaluation activities. The Scheme Owner also appoints suitably qualified Certification Bodies to perform the MDSCert product certification activities. The Scheme Owner maintains and manages the scheme operations and certificates during their lifetime and provides a terms and conditions framework to ensure consistency and compliance against the Scheme objectives and requirements.

Mobile Device Manufacturers can evaluate Mobile Device conformance to the requirements defined in the ETSI TS 103 732 series [2] and the GSMA MDSCert Security Requirements. Mobile device manufacturers that wish to have their Mobile Devices certified under MDSCert can indicate, to the Scheme Owner and a selected MDSCert Security Test Laboratory (MSTL), their intention to do so. They can then submit a completed questionnaire (the format for the questionnaire is up to the Scheme Owner) and select the level of security assurance they are seeking. Depending on the security assurance level being sought, the mobile device manufacturer engages with an MSTL to obtain the necessary evaluation services.

On receipt of all applicable documentation, mobile device specimens, etc., the MSTL will perform the necessary level of evaluation with support from the Mobile Device Manufacturer. When the evaluation is completed and the Evaluation Report has been agreed upon, the MSTL will submit the results to the MSCB.

The MSCB will review the submitted Evaluation Report and the MSTL recommendations and conclusions regarding compliance with the MDSCert Scheme security requirements and make the final decision on the certification award.

Successful certifications will be notified by the MSCB to the Scheme Owner and results and device details will be published following agreement with the Mobile Device Manufacturer. These details will be recorded in a publicly accessible registry that lists the Mobile Devices that have been certified and the applicable Security Assurance Level.

The Scheme Owner provides a process for accepting and resolving disputes pertaining to evaluations and certification, which is defined in Section 15.

The MDSCert Scheme has been designed with practicality and efficiency in mind to minimise duplicate effort for the benefit of all stakeholders. OEMs may accrue a number of different Mobile Device products under a common certificate provided those devices are derived from the same underlying device platform and the differences between those devices do not change or diminish the security of the underlying device platform. This is called Certification through Similarity. Mobile Device Manufacturers may also use security certificates obtained for their device, or components of their devices, from other public third-party schemes as evidence of compliance against some of the GSMA MDSCert security requirements.

Certificates issued against the MDSCert Scheme have a validity period of two years or less and the term is set by the scheme owner.

Products must be re-evaluated against the requirements of the Scheme to retain a certified status, given that the security requirements may evolve in line with the evolving threat landscape and to ensure in-life updates to products are being carried out. This is called Maintenance (see section 11). All prior results, which remain relevant, can be used as part of maintenance re-evaluations to make the certification process more efficient.

The MDSCert Scheme provides a process for accepting and resolving queries about compliance from external parties of previously evaluated/certified products and will update the certification status of Mobile Devices if that is necessary. The Scheme Owner may revoke a certificate if, after formal analysis, a Mobile Device product is found to no longer meet the security requirements of the MDSCert Scheme.

4 MDSCert Roles

The MDSCert scheme involves a range of actors that perform a variety of roles in support of the scheme. The roles of each participating actor are described below.

4.1 GSMA

GSMA, through the Device Security Group, sets the overall security requirements included in the Scheme and maintains the Scheme documents to be used by any prospective Scheme Owner. As the author and maintainer of the MDSCert Scheme, GSMA is responsible for:

- Managing and maintaining an industry group responsible for maintaining the Scheme requirements and its evolution.
- Maintaining and making available MDSCert Scheme documents.
- Managing market feedback process (where applicable for maintaining the Scheme).

4.2 Scheme Owner

An MDSCert Scheme Owner is responsible for the overall direction and operations of the Scheme. A Scheme Owner ensures necessary enablers are in place to support evaluations and certifications and maintains the website used to publish MDSCert Scheme certifications based on the MDSCert Scheme documentation. A Scheme Owner is responsible for:

- Participating in the GSMA industry group responsible for maintaining the Scheme requirements.
- Appointing competent Certification Bodies and ensuring their adherence to the MDSCert scheme requirements.
- Authorising competent Test Labs and ensuring their adherence to the MDSCert scheme requirements.
- Managing market feedback process.
- Managing the MDSCert scheme dispute resolution process.
- Publishing certification results and associated information, maintaining an archive of historical certification data and managing the changes in certificate status between Valid, Expired and Revoked.

4.3 Mobile Device Manufacturer

The Mobile Device Manufacturers submit mobile devices for evaluation according to the requirements laid out in the MDSCert scheme. The Mobile Device Manufacturer will:

- Agree to the terms and conditions of the relevant actors to participate in the Scheme.
- Submit products for certification under one or other MDSCert Scheme security assurance levels.
- Supply the required information and samples applicable to the chosen security assurance level and assist the MSTL and MSCB in the work of evaluating and certifying its Mobile Device products.
- Fulfil its obligations relating to its certified products during the validity period of its certificates and conduct any certificate maintenance requirements indicated by the product during its life.

4.4 MDSCert Scheme Certification Bodies

The MDSCert Scheme is designed to operate in accordance with the provisions and expectations of ISO/IEC 17065 [3]. The Scheme Owner appointed MDSCert Scheme Certification Bodies (MSCBs) are responsible for gaining and maintaining ISO/IEC 17065 accreditation to participate and provide certification services for the scheme, including

identifying necessary updates to ensure enduring MDSCert scheme alignment with ISO/IEC 17065 expectations and for agreeing to terms and conditions for participation in the scheme. The MSCB(s) shall specifically include the MDSCert scheme within the scope of their ISO/IEC 17065 accredited certification activities.

The MSCB(s) are responsible for, among other things, certification activities, authorising, supporting and monitoring the performance of MSTLs (according to the defined criteria in FS.54 [5] and FS.55 **Error! Reference source not found.**).

The primary point of contact information for the MDSCert scheme at each MSCB shall be published on the Scheme Owner's website, along with details of the MSTLs, as well as links to scheme procedures and documents. The Scheme Owner is responsible for oversight across MSCBs to ensure consistency across accreditations performed by the MSTLs under the different MSCBs.

4.5 MDSCert Scheme Test Laboratory

MSTLs are authorised to perform Mobile Device Evaluations by the MSCBs. For laboratories to become, and stay, authorised under the scheme, they need to:

1. Have and maintain a valid accreditation from:

    a) ISO/IEC 17025 accreditation with Common Criteria.
    b) a 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 [7].
3. Agree to terms and conditions for participation in the scheme.

Candidate MSTLs wishing to be authorised should contact the MSCB(s) and be prepared to provide evidence of how the above requirements are met. The result of a successful submission and authorisation is a listing by the Scheme Owner as a MSTL under the MDSCert scheme. Detailed requirements can be found in MDSCert Scheme Test Laboratory Accreditation [FS.54].

5 MDSCert Security Requirements

The MDSCert Scheme defines a set of security requirements that are derived from several sources, including existing sets of industry and government security requirements and interpretations of best practices.

These requirements have been grouped into the following categories:

- Cryptography.
- Updates.
- Preloaded applications and permissions.
- Authentication.
- User and privacy settings.
- Device integrity.
- Connectivity.
- Vulnerability remediation and patching.

- Device lifecycle.
- Device bootloader.
- Device security configuration.
- OTA client and updates.
- Device signing keys.

GSMA utilises the ETSI TS 103 732 series [2] as the primary reference for security requirements for Mobile Devices. Where the TS 103 732 series does not provide security requirements that cover all areas, GSMA will create supplemental documents to provide full coverage of the MDSCert requirements.

The MDSCert Scheme defines the specific version(s) of the ETSI PP that are applicable to the Scheme. Applicable versions are subject to change over the life of the Scheme.

As part of the Lifecycle requirements, the security assessment covers the Mobile Device Manufacturer's vulnerability and patch management policies. While there is no specific policy or threshold from the MDSCert Scheme for these policies to be considered a pass, the MSCB will assess such policies and processes against bespoken best practices. During a re-evaluation, the Mobile Device Manufacturer performance according to these practices will be reviewed.

Mobile device products meeting all these requirements will be awarded a MDSCert Scheme certification.

6 Security Assurance Levels

The MDSCert Scheme defines multiple security assurance levels to keep security requirements and assurance levels separate to provide the most flexibility (these levels have no relation to Common Criteria levels). These levels are hierarchical in that Security Assurance Level 2 encompasses all Level 1 requirements and then involves additional independent assessment by an MSTL. The Security Assurance Level indicates the degree to which the compliance of a Mobile Device to the MDSCert security requirements has been evaluated. Level 1 consists of a self-assessment by the Mobile Device Manufacturer and Levels 2 and 3 additionally include a Mobile Device Evaluation performed by an MSTL.

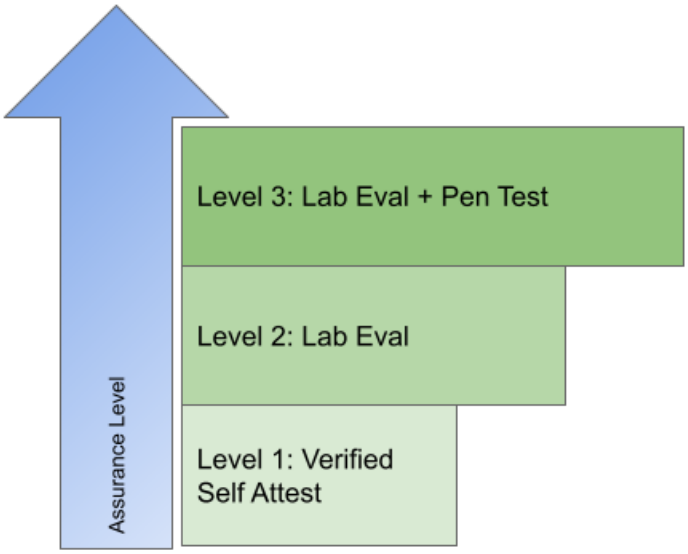

Figure 1 - MDSCert Assurance Levels

6.1 Security Assurance Level 1 (Verified Self-Assessment)

At Level 1, the Mobile Device Manufacturer is required to complete the self-assessment questionnaire and submit this along with any additional evidence (such as results from running test scripts that support the answers in the questionnaire). The information in the questionnaire is reviewed for completeness and if the information is considered complete, a certification would be awarded and published.

6.2 Security Assurance Level 2 (Functional Test + Documentation Review)

At Level 2, in addition to the evidence submitted for a Level 1 evaluation, the Mobile Device(s) shall be functionally tested to verify the claims in the questionnaire. The MSTL will verify the information in the questionnaire and any supporting evidence for accuracy. Once the claims of the Mobile Device Manufacturer have been verified as accurate and complete, a certification will be awarded and published.

6.3 Security Assurance Level 3 (Level 2 + Penetration Test)

At Level 3, in addition to the evidence submitted for a Level 2 evaluation and the functional testing performed by the MSTL, the MSTL will also perform a vulnerability assessment of the device, including penetration testing. Once the claims of the Mobile Device Manufacturer have been verified as accurate and complete and the penetration testing completed (with no penetrations to the specified attack potential), a certification will be awarded and published.

7 MDSCert Scheme Process

The MDSCert Scheme consists of the following stages:

1. Preparation.
2. Submission.
3. Evaluation.
4. Certification.

Differences between the Security Assurance Levels at each stage are defined in sections 7.1, 7.2, 7.3 and 7.4.

7.1 Preparation Stage

During the preparation stage, the Mobile Device Manufacturer:

- [ALL] Selects the Mobile Device product or products for evaluation and certification.
- [ALL] Selects the Security Assurance Level desired for each Mobile Device product.
- [ALL] Agrees to the terms and conditions of participation in the scheme with the Scheme Owner, MSTL and MSCB, as required.
- [ALL] Submits the completed application form.
- [SAL2/SAL3] Agrees on a time frame for the evaluation activities with the MSTL.

7.2 Submission Stage

During the submission stage, the Mobile Device Manufacturer compiles, completes and submits to the MSTL the following artefacts, as required by the Security Assurance Level being targeted:

- [ALL] the questionnaire.
- [ALL] any additional evidence documentation and artefacts.
- [ALL] any recognised security certificates relating to components.
- [ALL] any recognised security certificates relating to the product.
- [ALL] justifications of similarity.
- [ALL] recognised historical certification evidence for re-use.
- [SAL2/SAL3] product samples.

7.3 Evaluation Stage

The evaluation stage is defined in the MDSCert Scheme Security Evaluation Methodology (FS.55) and will be applied for Mobile Device Evaluations under the Scheme according to the Security Assurance Level applied for by the Mobile Device Manufacturer.

During the evaluation stage, the following actions occur:

- [ALL] The questionnaire is reviewed for completeness and accuracy.
    - [SAL1] An appointed MSCB or an authorised MSTL performs the review
    - [SAL2/SAL3] An MSTL performs the review.
- [SAL2/SAL3] MSTL runs (see note below) all functional tests on the physical devices to validate Mobile Device Manufacturer assertions from the test questionnaire.
- [SAL2/SAL3] MSTL reviews all Mobile Device Manufacturer submitted documentation to satisfy all of the non-technical requirements (i.e. security development lifecycle, flaw remediation, etc…).
- [SAL3] MSTL conducts penetration testing at AVA_VAN.2 (Basic Attack Potential) for designated requirements.

NOTE: The MSTL should execute all functional tests except under circumstances where it is necessary for the test to be handled by the Mobile Device Manufacturer and observed by the MSTL.

- [SAL2/SAL3] During the Evaluation, limited remediation work may be carried out by the Mobile Device Manufacturer in the event that a security requirement is not met by the Mobile Device product. See MDSCert Product Evaluation Methodology (FS.55) for further details.
- [ALL] Reporting of results and conclusions from Mobile Device Evaluations shall follow the requirements defined in the MDSCert Product Evaluation Methodology (FS.55).

7.4 Certification Stage

This stage addresses the scheme certification Review, Decision and Attestation functions. Upon the successful completion of the evaluation, the MSTL (or MSCB as may be appropriate at SAL1) prepares the Evaluation Report and sends it to the MDSCert CB. An evaluation that has stopped (such as one that may not be completed successfully for any reason) will not result in an Evaluation Report to the MDSCert CB; only a notice of the termination of the evaluation will be sent. The MSCB reviews the Evaluation Report evaluation results, the evaluation procedures and the testing methods applied by the MSTL. If the evaluation Report is produced by an MSCB, as may be appropriate at SAL1, it must be reviewed by a separate internal team at the MSCB.

During the MSCB report review, questions or comments from the MSCB on the Evaluation Reports should be directed to and addressed with the MSTL (or the MSCB team that performed the review). The MSTL (or MSCB team) can work with the MSCB (and, if necessary, the Mobile Device Manufacturer) to address any questions or comments (including, as needed, additional testing). Upon approval of the Evaluation Report, the MSCB prepares a Certification Report including the Certification result (pass or fail), which is delivered to the Mobile Device Manufacturer, the MSTL (or MSCB as may be appropriate for Level 1) and the Scheme Owner. Successful Certifications are published by the Scheme Owner and are designated “valid”.

8 MDSCert Scheme Certification Decision and Attestation

8.1 Certification Decision

Upon completion of the evaluation, the MSTL submits the evaluation technical report to the MSCB for its formal review. After the evaluation technical report approval, the MSCB prepares a Certification Report with a recommendation of certification which will be the base for the Certification decision. The MSCB is solely responsible for the Certification decision, which is documented in the certification report documentation. When formulating a Certification decision regarding Mobile Device compliance with the MDSCert scheme security requirements, the Certification decision shall be one of the following:

1. Certified: The Mobile Device fulfils the security requirements and is certified compliant.
2. Not certified: The mobile device is not compliant and not certified.

If the MSCB denies approval for Certification, it shall identify the reasons for not approving and communicate these in the Certification Report. The manufacturer shall be notified of the next steps. The Certification decision applies to the different certification processes including:

- Granting initial Certification.
- Extending or reducing the scope of Certification.
- Revocation of Certification.
- Maintenance of Certification.

8.2 Attestation

In case of a positive Certification decision, an MDSCert Scheme certificate is issued that describes the scope of the Certification, security assurance level and the validity period. Formal certification documents are issued and provided to the manufacturer only after approval of certification by the MSCB which includes:

- The Certificate.
- The Certification Report.

The Scheme Owner maintains a public list of current certificates where the timing of publishing is agreed with the Mobile Device Manufacturer. The Scheme Owner also maintains a public list of archived certificates including those that have expired (the manufacturer has not provided an update that would extend the certification expiration date) and those that have been revoked (where a MSCB has revoked a valid certificate according to the terms of the scheme).

All expired and revoked certificates are maintained in the public archive. The archive list provides historical context and information even if the certificates are no longer valid. Certificates that are archived (or removed at the request of a Mobile Device Manufacturer) can no longer be used to provide claims of Mobile Devices being compliant or certified in accordance with the MDSCert security requirements.

9 MDSCert Scheme Certification Scenarios

There are multiple certification scenarios for how an evaluation may proceed. Evaluations may cover only a single device model, variant, or a whole Product Family (and associated variants), as the Mobile Device Manufacturer may prefer. The following sections explain these scenarios and how evidence for meeting the requirements can be provided. The ultimate responsibility for ensuring Mobile Device models and variants are appropriately certified (whether through individual Certifications and/or via Certification by Similarity), ultimately rests with each Mobile Device Manufacturer and must be agreed with the MSTL and MSCB.

9.1 Single Mobile Device

In the most basic type of evaluation, a single Mobile Device is evaluated against the MDSCert security requirements in a single evaluation, where all requirements are reviewed and compliance is evaluated. The amount of review is determined by the SAL of the certificate being sought.

9.2 Multiple Mobile Devices and Similarity

Mobile Device Manufacturers may wish to evaluate a series of Mobile Device models (a Product Family) instead of a single product. An evaluation of similar Mobile Device models may occur at once (multiple similar device models evaluated at one time) or separated by time (a device model launched later with common components), in accordance with common principles. The Mobile Device used as the basis for all similarity comparisons is the Reference Mobile Device (RMD).

Similarity is defined by comparing a second Mobile Device to the RMD. If the security functionality is provided by the same components, then the two Mobile Devices are considered similar, and the second device may be certified without undergoing direct evaluation on its own.

Similarity shall, at a minimum, encompass the following examples:

- 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 - replaced/changed components from the RMD disallow certification by similarity for the new Mobile Device.

A Mobile Device submitted for Certification by similarity inherits the security claims of the RMD that has already been evaluated.

It is permitted that Mobile Device models submitted for evaluation by similarity are like a previously certified device and the new Mobile Device may contain updates (patches, security fixes, etc.) to the software or firmware from the initially evaluated RMD, as long as these do not violate the above rules. All differences in software (including preloaded apps) or firmware shall be described by the Mobile Device Manufacturer to enable the MSTL and MSCB to make an accurate comparison between the devices.

Similar devices may encompass changes to components not affecting security, such as the following:

- Colour.
- Enclosure.
- Language.
- Form factor.
- Screen.
- Battery.
- Input mechanisms.

To complete an Evaluation by Similarity, the following shall be provided by the Mobile Device Manufacturer:

- 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 equivalency analysis shall be submitted to the MSTL and MSCB as part of the submission phase. The MSTL shall perform a differential vulnerability assessment as part of the Mobile Device Evaluation and report the results of the updated analysis compared to the RMD evaluation.

The MSCB has the final decision on whether or not a Mobile Device qualifies for Evaluation by Similarity according to the process and criteria described above.

9.3 Mobile Devices, Composition and Reusability

In many cases, a Mobile Device will be made up of several components, such as hardware, software or firmware that may have been separately certified previously. This could range from the whole Mobile Device using a similar evaluation to an individual component providing a specific security function. The MDSCert Scheme facilitates the reuse of external certifications to provide efficiencies in how Mobile Device Manufacturers are able to obtain MDSCert scheme certification. While external certifications are not mandatory, they may also not be sufficient to meet the MDSCert Scheme requirements. Any external certifications shall be reviewed for appropriateness and any gaps that remain between those certifications and the MDSCert Scheme security requirements need to be addressed by the Mobile Device Manufacturer.

When using certified components and platforms, the MSTL may conclude that certain tests are no longer required and increase its time and effort on verifying the proper integration of the security functionality of the certified component or platform. Such decisions shall be justified in the evaluation report, supported by evidence backing up the rationale for the decision. Acceptable evidence can be a companion certificate from public and private schemes like CC or SESIP, as an example, describing the security functionality implemented by component and platform, as well as the secure integration guidance that the Mobile Device Manufacturer will need to follow to address vulnerabilities while relying on the provided security functionality. For example, the SoC or secure element can provide cryptographic capabilities certified under CC, having the laboratory focus on verifying that for the particular use case declared by the Mobile Device Manufacturer, the cryptography in use is indeed from the component and in accordance with the integration guidelines.
Composition and reusability procedures are detailed in GSMA FS.55 MDSCert Product Evaluation Methodology FS.55 [6]. Re-usability is appropriate in the following scenarios:

1. Multiple Mobile Device models included in a single evaluation contain common components. These components may only need to be evaluated on one Mobile Device model (the RMD for that component).
2. Mobile Device models seeking Certification based on their *similarity, as indicated by a minimum set of common characteristics as described in section 9.2,* to previously evaluated and certified RMD.
3. Mobile Device models seeking Certification have components which have been independently certified (with a public certificate), matching the Mobile Device under evaluation. The component certificate may be used to show compliance with its requirements.

In all of the scenarios where reusability of certification is sought, the MSCB has the final decision on whether or not a Mobile Device can be certified using evidence from other evaluations or certifications.

10 MDSCert Scheme Certificate Validity Period

The MDSCert Scheme certificate is valid for two years or less from the evaluation completion date and no longer than the remaining support period for a Mobile Device. The certificate validity period is set by the scheme owner. The Mobile Device Manufacturer may choose to demonstrate continuing compliance with the MDSCert requirements. There are three methods for demonstrating continuing compliance: a full re-evaluation, a maintenance evaluation and a targeted response evaluation. The three methods to extend the Certification of a Mobile Device are described in section 11. A Mobile Device can undergo regular Certifications and as long as the Mobile Device is able to continue meeting the Certification requirements, is able to be certified indefinitely.

11 MDSCert Certification Maintenance

A new evaluation of the Mobile Device will extend the validity period of the MDSCert Scheme certificate for another certificate validity period from the date of the completed evaluation (or from the end date of the previous certification if the Mobile Device had already started evaluation before the expiration of the previous certification). While the purpose of a full re-evaluation and a maintenance evaluation are the same, the differences are based upon the scope of changes to the Mobile Device since the last completed evaluation, and so the available evaluation options are determined by the changes as specified in section 11.1.

A targeted response evaluation provides evidence of compliance to the previous certification, showing the Mobile Device still meets those same requirements. A targeted response evaluation is intended to be more limited in scope, and does not change the validity period for the previous certification. Targeted response evaluations focus on changes made to the Mobile Device based on a specific issue that has been raised with the certification of the device. Most commonly a targeted response evaluation would be performed based on a Market Feedback challenge (section 14).

11.1 Product Changes and Certification Maintenance

During the lifecycle of a Mobile Device, it will undergo many changes. The type of changes will have an impact on the type of evaluations which may be required to maintain the certificate that has been awarded to the Mobile Device.

The following table categorises the Mobile Devices changes and the available options for re-evaluation. The Mobile device Manufacturer can choose to undergo a more complete evaluation (subject to the restrictions for each evaluation type) to maintain the Mobile Device certification.

Mobile Device Changes	Full Eval	Maint. Eval	Response Eval
Hardware changes – changing the Mobile Device hardware is considered as a new device.	X		

Mobile Device Changes	Full Eval	Maint. Eval	Response Eval
Significant software changes to the device or its components, such as Major OS version update, major firmware update – changing the primary version number of the OS or a major update to the firmware.	X		
Regular maintenance patches, minor OS version update – changes which do not modify the primary version number of the OS, including regular patching (as required by MDSCert).	X	X	
A patch targeting a specific reported issue on the Mobile Device (the patch may be included as part of a regular patch or out-of-band).	X	X	X

Table 1 - Mobile Device Changes

The Mobile Device Manufacturer shall provide a justification for how the changes to the Mobile Device justify the requested evaluation is appropriate. It is possible that cumulative small changes may justify a full evaluation instead of a maintenance evaluation. As changes are considered since the last evaluation, changes from a previous evaluation 3 months ago are more likely to be considered as minor than those from 10 months ago.

The MSTL and MSCB(s) have final say in the determination as to whether the requested evaluation type is appropriate.

11.2 Certification Maintenance through Product Re-evaluation

When the Certificate is set to expire, the only method for extending the validity period is to undergo a full re-evaluation of the Mobile Device. However, such re-evaluation may rely on the reuse of relevant evidence materials from a previous evaluation, such that the new evaluation (re-evaluation) may be quicker than the initial evaluation.

11.3 Certification Maintenance through Maintenance Evaluation

During the validity period of a Mobile Device Certification, there may be reasons for the Mobile Device Manufacturer to demonstrate continuing compliance to the MDSCert security requirements.

This type of evaluation is generally determined by the Mobile Device Manufacturer directly. For example, the Mobile Device Manufacturer may have a contractual obligation to demonstrate on a quarterly basis that the changes introduced by regular patching do not impact the security functionality of the Mobile Device. In this case, the Mobile Device Manufacturer may undergo a maintenance evaluation focused on the changes since the initial evaluation.

When the Mobile Device Manufacturer chooses to undergo a maintenance evaluation, the MSCB will be notified of the Certificate that is being updated and the Certificate will be (internally) marked as under review until the maintenance evaluation is complete.

If the maintenance evaluation is not completed successfully, the certificate is revoked (archived) as the Mobile Device is no longer considered compliant. If the maintenance evaluation is completed successfully, the certificate is updated to show the latest evaluation date (and identification of the current version of the Mobile Device and its components that were reviewed) and the certificate expiration is adjusted to the certificate validity period from the date of completion.

Failure to adhere to any of these requirements could lead to certificate revocation according to the rules outlined in the MDSCert Scheme terms and conditions.

When a Mobile Device certificate is to undergo a maintenance evaluation, there are different expectations based on the level of security assurance the product is certified to.

In all cases, the Mobile Device Manufacturer shall provide an updated questionnaire and a list of the changes from the most recently certified Mobile Device and any security claims they may resolve (for example a specific CVE being patched).

11.3.1 Level 1 Maintenance Evaluation

At this level, the Mobile Device Manufacturer shall attest it has tested the changes and verified they do not change the claimed functionality.

11.3.2 Level 2 Maintenance Evaluation

At this level, in addition to the Level 1 evidence, the Mobile Device Manufacturer shall provide the updated system image to the MSTL for review. The MSTL will review the changes to determine the impact of the changes on the product. Depending on the changes, limited functional testing may be required to verify the changes are compliant.

11.3.3 Level 3 Maintenance Evaluation

At this level, in addition to the Level 1 and 2 evidence, the Mobile Device Manufacturer shall provide a vulnerability analysis of the changes to the MSTL for review. The MSTL will perform an independent vulnerability analysis of the changes.

11.4 Certification Maintenance through Targeted Response Evaluation

During the validity period of a Mobile Device Certification, there may be reasons for the Mobile Device Manufacturer to demonstrate a response to a specific concern raised during Market Feedback regarding the MDSCert security requirements. To provide a method to support rapid Mobile Device Manufacturer response to in-market issues, the targeted response evaluation is focused specifically on the raised concern only.

In this case, an MSCB(s) has notified the Mobile Device Manufacturer of revocation due to a determination that the certified Mobile Device is no longer in compliance with the MDSCert security requirements. To maintain the certificate, the Mobile Device Manufacturer shall undergo a targeted response evaluation to demonstrate compliance with the MDSCert security requirements.

The difference with a targeted response evaluation compared with a full or maintenance evaluation is that it specifically only corrects the issue raised as making the device non-compliant with the certification requirements. A targeted response evaluation does not review any other aspects of the device (such as the latest patches applied since the last

evaluation); it only reviews the changes necessary to bring the Mobile Device back into compliance with the MDSCert security requirements.

A targeted response evaluation does not require any changes to the questionnaire (unless such a change is required to bring the Mobile Device into compliance).

If the targeted response evaluation is not completed successfully, the certificate is revoked (archived) as the Mobile Device is no longer considered compliant. If the targeted response evaluation is completed successfully, the certificate is updated to show the latest evaluation date (and identification of the current version of the Mobile Device and its components that were reviewed). A targeted response evaluation does not adjust the certification expiration date for the Mobile Device; it only prevents it from being revoked immediately.

12 MDSCert Scheme Certificate Revocation

The MSCB(s) manage the issuance and revocation of certificates under a defined MDSCert Scheme Certification policy. If a Mobile Device Manufacturer fails to follow the vulnerability and patch management policies declared at the time of the Certification for a particular Mobile Device that has been evaluated and certified, the certificate will be revoked.

When the Mobile Device Manufacturer has been informed of exploitable vulnerabilities and fails to address them, given they had adequate notice and time to analyse and fix them, in line with the mitigation timeframe specified in the policies reported by the Mobile Device Manufacturer at the time of the Certification, the certificate may be revoked by the MSCB.

When the Mobile Device Manufacturer fails to inform the MSCB of newly discovered exploitable vulnerabilities that impact a certified Mobile Device, thus denying awareness of such events, the certificate may be revoked. In the event that a Mobile Device Manufacturer’s conformance claims under the self-declaration process for Security Assurance Level 1 prove to be incorrect or inaccurate, the certificate for the certified Mobile Device may be revoked by the MSCB.

If the MSCB considers the responses from the Mobile Device Manufacturer to be a deliberate failure or violation of the terms under which the Certificate was awarded, the certificate may be revoked by the MSCB.

Revoked certificates are moved to the archive list by the Scheme Owner with the designation “revoked".

13 MDSCert Security Requirements Validity Period

The MDSCert security requirements are not static and will change over time as the capabilities of Mobile Devices change and new security functionality becomes available. Over time, a Mobile Device may cease to meet new security requirements (such as when a new hardware capability is added as mandatory), but this does not mean the certified Mobile Device is no longer secure in the context of the previous security requirements.

GSMA will regularly update the security requirements with new references and publications that will supersede earlier requirements. When this happens, there will be a transition period between the old and new requirement specifications. The transition periods for each

requirement specification update will be published on the GSMA MDSCert Scheme website as well as the implications and guidance for the Certification process.

Requirements have three stages to their lifecycle:

- CURRENT – these requirements can be used for any evaluation (new or maintenance).
- CONTINUITY – these requirements can only be used for maintenance evaluations on Mobile Devices that have already met these requirements.
- RETIRED – these requirements cannot be used for any evaluation.

When a new set of requirements is published, a transition period of one (1) year will start. During this transition period, there will be two sets of requirements that are CURRENT, and as such any evaluation can use either set. At the end of the transition period the older set of requirements will be listed as CONTINUITY and are not available for new evaluations.

The purpose of CONTINUITY is to allow for the continued certification of Mobile Devices which may not be able to meet newer security requirements, but which are still under active support to the security requirements which they have previously met. A certified Mobile Device which is unable to meet new requirements is able to maintain the certification to the last set of requirements until that set of requirements is moved to RETIRED status.

The time periods for these lifecycle stages are:

- CURRENT – this stage lasts until the end of the transition period after the publication of the next revision of the requirements.
- CONTINUITY – this state lasts for five (5) years.

These can be seen in the diagram below showing a nine year period (with the current time being around Year 5).

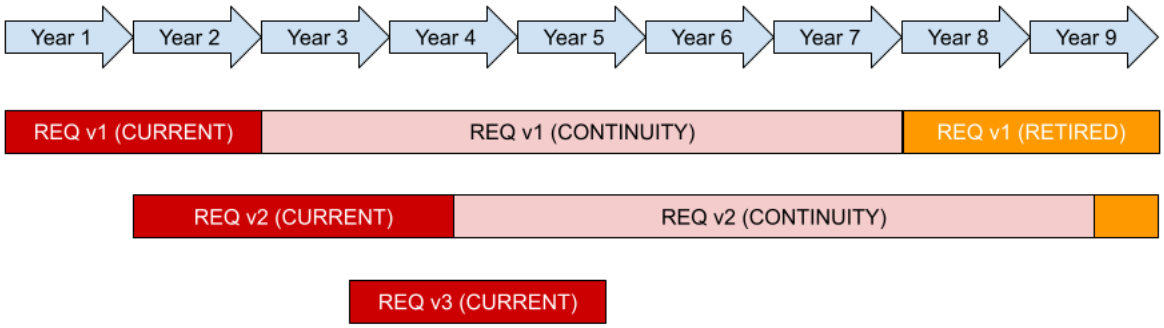

Figure 2 – Requirements Lifecycle

The diagram shows the transitions from CURRENT to CONTINUITY to RETIRED over the nine year period for REQ v1, REQ v2 and REQ v3.

Based on this guideline, a Mobile Device could be certified to the following requirements (per the start of each year):

- Year 1 – REQ v1 for any evaluation
- Year 2 – REQ v1 or REQ v2 for any evaluation

- Year 3 – REQ v1 only for maintenance evaluations if that is the most recent certificate, REQ v2 for any evaluation
- Year 4 - REQ v1 only for maintenance evaluations if that is the most recent certificate, REQ v2 and REQ v3 for any evaluation
- Year 5 - REQ v1 and REQ v2 only for maintenance evaluations if that is the most recent certificate, REQ v3 for any evaluation
- Year 8 – REQ v1 cannot be used for any evaluation

A Scheme Owner may choose to adjust the time periods for transitions between requirement versions and CONTINUITY over time.

14 MDSCert Scheme Post Certification Market Feedback Process

The MDSCert Scheme Owner will need to provide a mechanism for external entities to challenge the accuracy (and by extension, the validity) of a device Certification. Challenges shall be reviewed by the MSCB to determine the appropriate response actions. If the MSCB is unclear about or unable to determine a resolution, a Scheme Owner-established committee will make a final determination.

The MDSCert Scheme Owner will be responsible for the detailed process for handling market feedback, but the following outline provides a high-level description of the steps in the feedback process.

1. A challenge is submitted to the MSCB including sufficient information to properly identify the Mobile Device being challenged as well as evidence of non-compliance to the security claims made by the Mobile Device Manufacturer.

    a) Challenges with insufficient information for a complete analysis to be undertaken will not initiate the review process (additional information can be requested from the submitter before making this decision).

2. The MSCB shall perform an initial review of the evidence to determine whether the MSCB agrees with the challenge and that the certificate may be invalidated, a “Valid Challenge”.

    a) If the MSCB does not agree with the challenge, a response will be made to the submitter with the reason for rejecting the challenge.

3. For a Valid Challenge, the MSCB shall contact the Mobile Device Manufacturer and the MSTL to notify them of the challenge and the reasoning for the initial determination.
4. The Mobile Device Manufacturer is able to provide a response to the Valid Challenge.
5. Based on the Mobile Device Manufacturer’s response, a final determination of the challenge will be issued (such as changing the initial determination, considering the challenge valid but resolved, or considering the challenge valid and unresolved).

Some example responses from the Mobile Device Manufacturer when presented with a Valid Challenge may include:

- A counterargument against the validity of the challenge.

- A patch along with an expected release date (the update the patch would be included in).
- A plan for meeting the challenged claim (for example, more frequent updates where the update frequency was not met).
- A request to change the security claim for the device (such as changing the update frequency to a longer time period).

Some examples of the MSCB outcome from the analysis of the Mobile Device Manufacturer response are:

- Changes the initial validity determination of the challenge, in which case the Mobile Device Certification remains valid.
- Resolves the reported non-compliance, in which case the Mobile Device Certification remains valid while the manufacturer performs the remedial action by the due date. In the event the due date expires without remediation, the Mobile Device certificate is revoked.
- Requests further changes based on the response not being considered adequate to resolve the challenge.

The MSCB may revoke the MDSCert Scheme certificate related to challenges when:

- The Mobile Device Manufacturer is unable to provide an adequate resolution to the challenge (the MSCB does not consider the resolution to close the challenge and the Mobile Device Manufacturer is unwilling or unable to provide a further change).
- The Mobile Device Manufacturer fails to respond to the challenge inquiry from the MSCB.

In cases where the MSCB is unable to determine if the challenge inquiry should be considered valid (such as when an interpretation of the security claims may be unclear based on the challenge vs. previous expectations), the MSCB shall ask for guidance from the Scheme Owner.

14.1 Challenge Constraints

As it is expected that the Market Feedback Process will be quick and easy to use, any challenge process shall include safeguards to prevent abuse that may tie up resources of the Scheme Owner, MSCB, MSTL or Mobile Device Manufacturers on invalid challenges. While the MSCB initial review process should be sufficient to filter most insincere challenge attempts, the following guidelines should assist in limiting abuse.

- An organisation cannot submit challenges for the same issue more than once. Second attempt challenges should be rejected.
- Mobile Device Manufacturers cannot challenge other Mobile Device Manufacturers unless the challenge is reported specifically by a group within the Mobile Device Manufacturer that publishes security/vulnerability issues.

15 MDSCert Scheme Dispute Resolution Process

The MDSCert Scheme Owner shall implement a dispute resolution process to handle disputes that may arise with regard to the implementation and/or interpretation of MDSCert

Scheme documentation that could be subject to disagreements between two or more parties. The Scheme Owner may also discuss questions with the Device Security Group to clarify issues about the MDSCert Scheme documentation.

15.1 Dispute Resolution Process Example

This section is an example of how the GSMA proposes establishing a Dispute Resolution Process (DRP) and Dispute Resolution Committee (DRC) based on other schemes within the GSMA.

The MDSCert DRC shall be appointed on a per dispute basis to ensure each dispute is handled in a non-partisan manner.

Disputing parties shall use all resources reasonably available to resolve disputes before involving the MDSCert DRC.

Subject to the above, the Scheme Owner shall only be contacted if there is a dispute between two or more parties with respect to the interpretation and implementation of MDSCert procedures or documentation.

The MDSCert DRP can be invoked by the requesting parties sending a written request (e-mail) to the appropriate Scheme Owner designated contact who, upon review, will forward the written request to all other parties involved in the dispute, giving all the respondent parties the opportunity to comment on the wording of the invocation.

Upon the opportunity for parties to comment, if the dispute cannot be resolved within a period of no more than twenty (20) calendar days:

1. The requesting party may invoke the MDSCert DRP; and
2. All parties concerned are asked to supply all arguments and points of view in relation to the matter to the Scheme Owner. The Scheme Owner in turn will supply the same to the respective MDSCert DRP upon its formation.

At the time of invoking the MDSCert DRP, the Scheme Owner should determine if a similar dispute has been previously resolved by a MDSCert DRC ruling. If such a dispute has previously been ruled on and published, the affected parties may decide to follow the decision made.

For each dispute, the MDSCert DRC may for example consist of three individuals who have not been directly involved in the matter and who are not employees of entities that may be affiliated either with the appellant or a respondent company group, appointed as follows:

The appellant(s) shall appoint one impartial member of the MDSCert DRC. The named respondent(s) shall also appoint one impartial member. When more than one respondent is named, the respondents will collectively agree on the appointment of a single member. The appellant and the respondent(s) shall each identify their appointed panel member within five (5) business days of the Scheme Owner’s determination that a hearing is necessary. The two members so selected by the parties shall then appoint the third member; this appointment of the third member shall occur within ten (10) business days of the determination that an adjudication is necessary.

Disputing parties shall use all resources reasonably available to resolve disputes before involving the MDSCert DRC. All parties involved should identify the disputed issue(s) in advance in order to have a common understanding of the issue(s). All parties involved in the dispute should agree on the wording of the MDSCert DRC invocation, including the time at which the issue causing the dispute occurred.

For the purpose of the MDSCert DRP, the Scheme Owner will, to the extent available and accessible, provide to the appellant and respondent the relevant MDSCert scheme documentation in effect at the time of the dispute. Later versions of these documents may also be considered upon request if relevant to the dispute.

The MDSCert DRC shall proceed according to the MDSCert DRP and may provide additional guidelines and/or define further proceedings as it may deem necessary for the achievement of a resolution. The MDSCert DRC will use reasonable commercial efforts to seek to resolve disputes as soon as practical and without undue delay (normally within ten (10) days of the notification). A majority decision shall then be made by the MDSCert DRC members.

The Scheme Owner is responsible for the distribution of the MDSCert DRC ruling/decision in writing.

The MDSCert DRC ruling/decision is binding between the Parties involved in the MDSCert Dispute Resolution Process at the time of the dispute as agreed during the invocation of the MDSCert Dispute Resolution Process.

Rulings/decisions of the MDSCert DRC could vary in terms of their nature and severity and could result in sanctions such as the revocation of product evaluations held by Mobile Device Manufacturers or MDSCert scheme Test Laboratory accreditations and authorisations. Sanctions to be imposed, if any, are entirely a matter for the MDSCert DRC to decide on.

Any ruling/decision of the MDSCert DRC may be anonymised, shared with the MDSCert Scheme Oversight Board and used as an example for improving the current MDSCert scheme as long as it is not attributable to a particular involved party.

Note: In the event that a need to change MDSCert documentation has been identified as a result of the decision, the MDSCert DRC shall refer the case to the Scheme Owner, which should provide the information to GSMA's Device Security Group to develop the appropriate change request and propose it to the relevant document approval authority.

The MDSCert DRP shall be administered and documented by the Scheme Owner, as the Scheme Owner deems appropriate.

15.1.1 Possible Dispute Scenarios

The Scheme Owner does not assess, review, or interpret Evaluation Reports in any way. The Scheme Owner keeps the Evaluation Report confidential in case a dispute is filed by an involved stakeholder, which could lead to the invocation of the MDSCert DRP. Should any involved party see the need to challenge any decision of an MSTL or an MSCB, it may refer the matter to the MDSCert DRP. The following table illustrates a number of possible dispute

scenarios that could arise that involve a variety of parties. The table merely captures example scenarios and is not intended to be exhaustive.

	Mobile Network Operator	Mobile Device Manufacturer	MDSCert Test Lab	MDSCert Cert Body	MDSCert Scheme OB
Mobile Network Operator					
Mobile Device Manufacturer					
MDSCert Test Lab					
MDSCert Cert Body					
MDSCert Scheme Oversight Board					

Table 2 - Example Dispute Scenarios

15.1.2 Matters Outside the Scope of MDSCert DRP

The MDSCert DRP only deals with disputes in respect to the interpretation and implementation of MDSCert or its documentation. Any dispute with regards to the facts, findings or recommendations of an evaluation report should be resolved between the respective MSTL, MSCB and Mobile Device Manufacturer.

15.1.3 Liability of MDSCert DRC Members

Any ruling by an MDSCert DRC is undertaken “as is” with no liability (e.g. for the correctness nor for any damages caused by or resulting from any decision/ruling made by the MDSCert DRC) to the Scheme Owner, any MDSCert DRC members, Scheme Owner staff members or MDSCert Scheme Oversight Board or Scheme Owner members.

As a condition to invoking the MDSCert DRP, the appellant agrees to hold the Scheme Owner and the aforementioned individuals involved in rendering a ruling/decision harmless from any and all liabilities or damages arising from or related to the appellant’s invocation of the MDSCert DRP and associated matters.

16 MDSCert Certificate Description

The MDSCert Certificate shall contain the following minimum information:

- Product name for the application device(s).
- Unique identifier as established by the certification body issuing the certificate.
- Unique identifiers for the evaluated device(s).

- OS version of the Mobile Device.
- Name, address and contact information of the Mobile Device Manufacturer.
- Name, address and contact information of the MSTL that performed the evaluation.
- Name, address and contact information of the Certification Body that issued the certificate.
- Date the evaluation was completed.
- Period of validity of the certificate.
- Version of the Scheme security requirements.
- Security Level of the evaluation.

The Scheme Owner may require additional information.

Annex A Document Management

A.1 Document History

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

A.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.

A.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.