Mobile Device Security Certification Scheme - Evaluation Methodology

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 describes the Mobile Device Security Certification (MDSCert) Scheme Evaluation Methodology.

1.1 Scope

The evaluation methodology establishes how the product and evidence evaluation is done at the procedural and operational level. It is provided to assist Mobile Device Manufacturers and the MDSCert Security Test Laboratories in the performance of those activities.

1.2 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.

1.3 Definitions

Term[1]	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 GSMA appointed MDSCert Scheme Certification Body
Certification	The granting of a certificate for a Mobile Device that has been subjected to a Mobile Device Evaluation
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 (ETSI TS 103 732 series [2]) and the GSMA MDSCert Security Requirements.
Component	Any module, hardware or software, which can be considered discrete, and is used to support a security function being claimed as part of a Mobile Device Evaluation. A component may be made up of its own components.
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 Test Report	The report created by the MDSCert Security Test Laboratory with 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 Security Test Laboratory

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

Term[1]	Description
False Accept Rate	Proportion of verification transactions with wrongful biometric claims of identity that are incorrectly confirmed.
False Reject Rate	Proportion of verification transactions with truthful biometric claims of identity that are incorrectly denied.
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]).
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 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 (ETSI TS 103 732 series [2]) and GSMA MDSCert Security Requirements.
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.
Questionnaire	Simplified term for the complete set of documents required to show compliance to the MDSCert Scheme 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.

1.4 Abbreviations

Term	Description
3GPP	3rd Generation Partnership Project
ALC	Access Control List
CVSS	Common Vulnerability Scoring System
CC	Common Criteria

Term	Description
EAL	Evaluation Assurance Level
ETSI	European Telecommunications Standards Institute
FAR	False Acceptance Rate
FRR	False Rejection Rate
GSMA	GSM Association
HW	Hardware
IEC	International Electrotechnical Commission
ISO	International Standards Organisation
MDSCert	Mobile Device Security Certification Scheme
MSCB	MDSCert Scheme Certification Body
MSTL	MDSCert Security Test Laboratory
NIST	National Institute of Standards & Technology
NIST CAVP	NIST's Cryptographic Algorithm Validation Program
NIST CMVP	NIST's Cryptographic Module Validation Program
OS	Operating System
NVD	National Vulnerability Database
OTA	Over The Air
PP	Protection Profile
SAL	Security Assurance Level
SBOM	Software Bill Of Materials
SESIP	Security Evaluation Standard for IoT Platforms
SFR	Security Functional Requirement
SSH	Secure Shell Protocol
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TOE	Target of Evaluation

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
[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

Ref	Doc Number	Title
		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.
[6]	N/A	“Common Criteria CC:2022 Release 1”. Available at https://www.commoncriteriaportal.org/cc/
[7]	N/A	“Common Vulnerability Scoring System v3.1”, June 2019. Available at https://www.first.org/cvss/v3.1/specification-document
[8]	N/A	“Protection Profile for Mobile Device Fundamentals, v3.3”, PP_MDF_V3.3. Available at https://www.niap-ccevs.org/Profile/Info.cfm?PPID=468&id=468
[9]	N/A	OWASP MAS. Available at https://mas.owasp.org/
[10]	N/A	NIST ACVP Protocol supported list – Available at https://pages.nist.gov/ACVP/#supported
[11]	N/A	SOGIS Crypto WG Agreed Cryptographic Mechanisms. Available at https://www.sogis.eu/uk/supporting_doc_en.html
[12]	ISO/IEC 18033-1:2021	"Information security - Encryption algorithms Part 1: General" ISO/IEC 18033-1:2021 Available at https://www.iso.org/obp/ui/en/#iso:std:iso-iec:18033:-1:ed-3:v1:en

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 Manufacturer Evaluation Artefacts

According to the assurance levels and activities to be performed for Mobile Device Evaluations, the following evaluation evidence and information shall be made available by the Device Manufacturer to the MDSCert Security Test Laboratory (or the MDSCert Scheme Certification Body as may be appropriate):

1. [All levels] :
    - Filled out questionnaire (this may include a combination of both public and confidential information)
2. [Levels 2 & 3]:
    - Devices for evaluation

The questionnaire will be published as part of the certification. Since the questionnaire includes requirements that cover information that would be considered confidential, it is acceptable that confidential information be provided in a separate document. The public questionnaire though shall contain a high-level answer to every question, and the MSCB has final decision on whether the amount of information provided in the public questionnaire is sufficient.

Where multiple devices are evaluated together, justification about the similarities (such as common hardware or software components) shall be provided as part of the questionnaire so the MDSCert Security Test Laboratory can determine how to assess the devices, and their similarity, using these components.

The documentary evidence shall be provided to the Evaluators in English.

Incomplete information provision will result in an unsuccessful evaluation and certification outcome.

2.1 Questionnaire [All Levels]

The questionnaire shall respond to the full list of requirements for MDSCert, defined in the TS 103 732 series of documents and referenced in the GSMA MDSCert Security Requirements. The questionnaire shall be completed based on a current set of applicable requirements from the MDSCert Scheme at the date of the application for evaluation.

When a certification is successfully completed, the completed questionnaire will be made publicly available by the Scheme Owner along with the certificate. The Mobile Device Manufacturer shall provide the necessary confidential or proprietary information as supplemental evidence with high level summaries provided in the questionnaire.

The questionnaire shall include a self-assessment by the Mobile Device Manufacturer of how the Mobile Device complies with the MDSCert defined security requirements. The Mobile Device Manufacturer shall guarantee the completeness and accuracy of the questionnaire in accordance with the terms and conditions governing their participation in the scheme.

When multiple devices are evaluated together as part of a Certification by Similarity, the Mobile Device Manufacturer shall provide a justification on the appropriateness of the reuse of evidence between devices, with tables describing the similarities/differences between the Mobile Devices along with how these meet the MDSCert security requirements.

The self-assessment shall consider each individual security requirement, describing how Mobile Device Manufacturers have supported their assessment, based on:

- Rationale based on design concepts on how each security requirement is met and implemented.
- Evidence from testing (where applicable to produce necessary evidence for the Certification) performed by the Mobile Device Manufacturer.
- Conformance to another standard by the device or a component as evidenced by applicable certificates including justifying how the certificate is applicable to specific MDSCert security requirements (see Composition).

Testing performed directly by the Mobile Device Manufacturer shall provide sufficient detail for the MDSCert Security Test Laboratory (or MDSCert Scheme Certification Body as appropriate) to verify that the tests accurately verify the implementation and the Mobile Device meets the MDSCert security requirements. External testing to other standards shall have results publicly available that can be verified by the MSTL. The Mobile Device Manufacturer shall explain how the external testing demonstrates compliance with the MDSCert security requirements. The MSTL shall reject the test evidence if it is unable to confirm that it demonstrates a Mobile Device's compliance with a specific MDSCert security requirement.

The questionnaire addresses the following:

- all the SFRs of the ETSI TS 103 732-1 [2].
- and ETSI TS 103 732-2 for biometrics [2].
- GSMA-specific requirements based on the operating system of the device.

2.1.1 Mobile Device-Related Documentary Evidence, Public & Confidential

The questionnaire shall contain sufficient information so that, when read without any confidential information, it would be clear that the MDSCert security requirements are met (even though details may be missing). Many, if not most of the MDSCert security requirements can be answered with public information. Confidential information does not have to be provided in a specific format, but in the interest of efficiency should be provided in a manner which makes it clear which MDSCert security requirements the information is tied to. One example of this could be a second questionnaire that contains only the confidential information (or references to additional documents).

For the purpose of enhancing the Evaluator's knowledge of the Mobile Devices to be evaluated, and to demonstrate fulfilment of the MDSCert security requirements, the documentary evidence shall contain the following information (no particular format or documents are required) in support of each of the Mobile Device Manufacturer's claims:

- List of hardware Components. The list shall include the Mobile Device itself and the Components that provide security functionality being claimed by the Mobile Device Manufacturer. These Components are expected to be certified parts whose certificates are being submitted as proof of fulfilment of a MDSCert security requirement.
- List of software Components. This list shall include the software Components that support the security functionality being claimed by the Mobile Device Manufacturer. This could be provided by a Software Bill of Materials (SBOM) in a commonly used and machine-readable format.
- Functional specification that shall describe programming or user interfaces and how those interfaces provide the security functionality claimed by the Mobile Device Manufacturer.
- Process, policy, procedure, architectural and design documentation such as:
    - the device security architecture.
    - key hierarchy.
    - Device security policies (seccomp, SELinux or similar).
    - software stack.

  - hardware related interfaces.
  - Separate Execution Environment(s) on the device (such as TEE, secure element, Secure Enclave or similar).

- Configuration data such as kernel defconfigs, bootloader configurations, etc.
- Component test procedures.

In addition, the following information may be included to support the evaluation, but is not mandatory:

- Mobile Device Manufacturer tools for performing some types of tests (such as cryptographic algorithm testing)
- Source code listings, samples, and repositories
- Evidence from other relevant evaluations or independent assessment reports (such as for privileged applications, trusted applications or OTA update services) submitted for re-use. This type of evidence shall be clearly documented and is subject to MDSCert Scheme Certification Body approval. See Composition for more information about what is acceptable evidence.

2.1.2 Other Documentary Evidence and Testability

Some MDSCert security requirements are not functional and so not testable on the Mobile Device, but are related to the lifecycle (such as vulnerability management or some manufacturing requirements). These are generally marked with ALC in the MDSCert identifier and require documentation to prove the requirements are met.

Additional MDSCert security requirements may not be able to tested directly (such as low-level hardware functions, or certain types of failure modes which may require destructive testing). These requirements shall have documentary evidence provided to prove compliance.

In both cases, the MSTL shall review the evidence to determine whether it is sufficient to prove compliance and provide a justification as to this determination to the MSCB as part of the Evaluation Test Report. The MSCB has final approval in determining whether the provided evidence is sufficient to claim compliance.

2.1.3 Re-use of Results of Previous Evaluations of Similar Devices

The re-use of previous evaluation results is defined as the use of a previously generated evaluation report for a security requirement issued by an authorised MSTL for the same or Similar device as evidence for a new evaluation.

The re-use of the previous evaluation results shall be justified by the MSTL to the MSCB in the Evaluation Report.

The conditions where the results of previous evaluations are applicable for new evaluations is covered under the composition and maintenance sections.

2.1.4 Implementation Representation

Where it is not feasible to perform direct testing of a Component to verify compliance with the security claims, the Mobile Device Manufacturer can provide an implementation

representation (e.g. source code / HW drawings) as evidence for the MSTL to review. In these cases, implementation representation reviews need to be accepted by the MSCB for verification instead of testing compliance with the requirement.

The implementation representation shall define the security functionality to a level of detail such that it can be generated without further design decisions (for example, directly compiled into an application used on the Mobile Device).

The implementation representation may be submitted in a proprietary form used by the Mobile Device Manufacturer. However, information provided which cannot be comprehended by the MSTL, or the MSCB, will result in an unsuccessful certification outcome.

2.2 Devices for Evaluation

The Mobile Device Manufacturer shall provide the Mobile Devices for the evaluation along with instructions about how to prepare the Mobile Devices for testing.

Acceptable Mobile Devices are:

- Final Production models
- Late Engineering models
    - These models shall encompass the same hardware components as the Final Production models but may have different shells and may also have the ability to load engineering or debug-capable system images.

Unacceptable Mobile Devices are:

- Early Engineering models
- Prototypes

Devices that are not in the final configuration used for public manufacturing are unacceptable Mobile Device models.

Mobile Devices provided for testing shall be capable of performing rollback firmware testing (this will require firmware packages that provide higher and lower version numbers to test with).

To support Level 3 evaluations, Mobile Devices that can be configured to provide root or debug access may be necessary.

3 Evaluation Methodology

The three security assurance levels of the MDSCert Scheme generate different levels of output corresponding to the activities mandated at each level. The table below provides an overview of the evaluation output based on the security assurance level.

Level	Evaluation Report Content
Level 1	Evaluation Technical Report
Level 2	Evaluation Technical Report

Level	Evaluation Report Content
	Questionnaire evaluation report Functional testing report
Level 3	Evaluation Technical Report Questionnaire evaluation report Functional Testing report Vulnerability Analysis and Penetration Testing Report

Table 1- Evaluation Report Level Content

The evaluation process and the activities that go into generating the content needed for each of these reports are described in the following sections.

3.1 Evaluation Process

Once a manufacturer has provided the required evidence artefacts for the Level of Certification they have applied for, the MSTL (or MSCB as may be appropriate) takes the following steps:

- Makes an initial review of the material.
- Requests any missing or additional material from the Mobile Device Manufacturer required to complete the evaluation (to be provided within the agreed time limit).
- In the event that an Evaluation Activity outcome is Fail, informs the Mobile Device Manufacturer who then has the option of:
    - Withdrawing from the evaluation process
    - Providing mitigation(s) or resolution(s)
- Compiles the Questionnaire Evaluation Report, the Functional Testing Report and, where applicable, the Vulnerability Analysis and Penetration Testing Report and submits it to the MDSCert Scheme Certification Body.
- In the event the MDSCert Scheme Certification Body's assessment results in a Certification Fail, the MDSCert Scheme Certification Body informs the Mobile Device Manufacturer who then has the option of:
    - Withdrawing from the evaluation process.
    - Providing mitigation(s) or resolution(s).
- In the event the MDSCert Scheme Certification Body assessment results in Certification, the results are passed to the Mobile Device Manufacturer for its records and to the Scheme Owner for publishing.

3.2 Evaluation Activities

The duration of the various MDSCert evaluation activities is ultimately defined in the MDSCert Scheme terms and conditions defined by the MSTL, MSCB and Scheme Owner that are agreed with the participating Mobile Device Manufacturers. These terms may include service level agreement targets and rules for extensions or remediation work. As a rough guide, the maximum duration of MDSCert evaluations is expected to take in the region of:

- Level 1, 3 weeks.
- Level 2, 9 weeks.
- Level 3, 13 weeks.

If, during the evaluation process, the Mobile Device Manufacturer needs to request additional time to successfully complete the evaluation, a pause in the evaluation may be requested, subject to agreement by the MSTL and MSCB. This can provide the Mobile Device Manufacturer with the time necessary to complete remediation for failures that may be reported during the evaluation process (instead of withdrawing from the evaluation).

3.3 Evaluation Reports

There are four separate reports that may be generated in an evaluation. The specific reports depend upon the SAL of the evaluation. Each report contains a number of pre-defined sections which shall be completed by the Evaluator.

3.3.1 Questionnaire Report

The Questionnaire Report shall contain the following sections:

1. Introduction:
    - Identify the Mobile Devices under evaluation.
2. Questionnaire review results:
    - PASS/FAIL results for all MDSCert requirements.
3. Conclusion:
    - Final recommendation based on the information provided in the questionnaire.
4. Bibliography:
    - Reference list to all information used in the evaluation process.

3.3.2 Functional Testing Report

The Functional Testing Report shall contain the following sections:

1. Introduction:
    - Test objectives and summary.
2. Test platforms and environments:
    - TOE version information (detailed).
    - Test environment.
    - Testing tools.
3. Test case description:
    - Description of each individual test and outcome of the test.
4. Conclusion:

- Final recommendation based on the results of the functional testing.

3.3.3 Vulnerability Analysis and Penetration Testing Report

The Vulnerability Analysis and Penetration Testing Report shall contain the following sections:

1. Introduction:
   - Test objectives and summary.
2. Vulnerability analysis and penetration testing strategy.
3. Test platforms and environment:
   - TOE version information (detailed).
   - Test environment.
   - Testing tools.
4. Public vulnerability search:
   - Keywords, search terms, findings in NVD.
   - Descriptions of excluded vulnerabilities.
   - Table with findings.
5. Independent vulnerability analysis:
   - Analysis of identified vulnerabilities.
6. Penetration test description:
   - Description of test, expected outcome, actual outcome.
7. Conclusion:
   - Final recommendation based on the results of the vulnerability analysis and testing.
8. Bibliography:
   - Reference list to all information used in the analysis.

3.3.4 Evaluation Technical Report

The Evaluation Technical Report shall contain the following sections:

1. Introduction.
2. Manufacturer information and TOE reference.
   - TOE version information (detailed).
3. Evaluation Result
   - Summary of questionnaire review result.
   - Summary of functional testing result.
   - Summary of vulnerability analysis and penetration testing result.

4. Overall verdict.
5. Lab recommendations.
6. Bibliography.

3.3.5 Assessment Verdicts in the Technical Reports

All Technical Reports contain the verdicts for the MDSCert security requirements (as appropriate to the Technical Report). While the final versions of the Technical Reports may only include PASS or FAIL verdicts, interim reports may also include INCONCLUSIVE verdicts.

For the Mobile Device Manufacturer to successfully complete the MDSCert evaluation, the Technical Reports can only include PASS verdicts for the individual requirements. Generally, the Mobile Device Manufacturer is expected to correct any issues that result in a FAIL or INCONCLUSIVE verdict such that the Mobile Device will receive a PASS verdict for the completion of the evaluation.

During the evaluation process, the MSTL would provide the Mobile Device Manufacturer with updates about interim verdicts so they can be remediated as necessary. The MSTL shall determine whether a remediation is sufficient to change the verdict to a PASS.

When a remediation is provided to resolve a non-PASS verdict, the Mobile Device Manufacturer shall provide an explanation of the scope of the remediation so the MSTL can determine whether additional re-testing may be required in case the change impacts other aspects of the security claims under review. Insufficient information from the Mobile Device Manufacturer may lead to longer test times or a continued FAIL verdict.

4 Evidence Assessment

4.1 Questionnaire Assessment

The assessment of the questionnaire submitted by the Mobile Device Manufacturer, by the MDSCert Scheme Certification Body, shall determine if it is complete, consistent and accurate providing information on compliance for all requirements:

- Completeness:
    - The Evaluator shall check that the information uniquely identifying the devices for certification has been included. The devices shall be uniquely identified.
    - The Evaluator shall check that all MDSCert security requirements have been addressed by specific security functions and that the necessary supporting evidence has been submitted.
    - In the event that the Mobile Device Manufacturer considers that a security requirement is not applicable to a Mobile Device, given its purpose or available interfaces, the Mobile Device Manufacturer shall provide a justification. The MSCB shall make a determination whether each such claim (and omission of evidence) is compatible with the scheme and enables the Mobile Device to be certified subject to successful outcomes of the other activity evaluations.
- Accuracy:

  - The Evaluator shall check that the information provided by the Mobile Device Manufacturer is accurate compared with the results of functional testing performed during the evaluation.
  - The Evaluator shall check that the descriptions faithfully describe what is implemented.

- Consistency:

  - The Evaluator shall check that the information does not provide divergent or conflicting answers to separate security requirements.

4.2 Additional Evidence Assessment

The purpose of this activity is to review applicable third party provided documentary evidence in the form of certificates, with justifications required to demonstrate compliance with Mobile Device Manufacturer nominated security requirements.

The assessment of the supporting evidence may be applied to the following activities:

- Examine/verify information regarding the Devices for Certification.
- Examine/verify ETSI TS 103 732 [2] series SFRs.
- Examine/verify Biometric Requirements.
- Examine/verify Life Cycle Requirements.
- Examine/verify GSMA MDSCert Security Requirements.

The document review activity shall be carried out by the Evaluator to check that the content is sufficient to justify the fulfilment of the claimed security requirement(s).

4.2.1 Preloaded Application Assessment Results

Of all the requirements, the ones related to preloaded applications are most difficult to readily quantify with a verdict. Mobile Devices may typically contain a large number of preloaded applications (potentially hundreds) to support the expected functionalities of a Mobile Device. While each individual preloaded application has its own results, the output from this is difficult to present in a meaningful manner. Note that the MDSCert scheme is meant to assess the overall security of the mobile device itself rather than the security of applications considered individually, and that applications downloaded with user consent post-issuance are not included, The OWASP MAS [9] community has created a method for evaluating the results of application checks and then presenting a combined score that represents the overall risk of the applications based on a set of parameters. The result of this work from OWASP MAS is to provide a meaningful way to assess a group of applications with a single score that can represent this risk.

Using the combined results from all the preloaded application reviews, the OWASP MAS [9] scoring formula is able to provide an overall assessment result for the Mobile Device. The individual data generated by the preloaded application testing shall be included in the overall report package (supplementary materials such that the score could be generated independently and verified), while the score based on the OWASP MAS [9] formula is reported as part of the questionnaire report.

This result is not reported as a PASS/FAIL, but as the score only.

4.3 Assessment Verdicts

A PASS verdict will be awarded if the supporting evidence provided by the Mobile Device Manufacturer allows the MSTL to assess if the objectives and security requirements have been met.

An INCONCLUSIVE verdict may be assigned for intermediate partial reports to inform the Mobile Device Manufacturer that the information provided is insufficient to meet the objectives. See Evaluation Methodology for more information about remediation.

A FAIL verdict will be awarded if the supporting evidence provided by the Mobile Device Manufacturer causes the MSTL to conclude that the objectives and security requirements have not been met.

The Preloaded Apps assessment is presented as the overall risk score (not as PASS/FAIL).

Only [PASS/FAIL] verdicts and the Preloaded Apps score will be presented in the final reports.

4.4 Evaluation Reports

The Evaluator shall prepare a technical report with a summary of the results of the analysis of the level of compliance of the Mobile Device with the MDSCert security requirements, assessing whether the Mobile Device Manufacturer has accurately justified the claimed compliance with each requirement.

5 Functional Testing

To facilitate functional testing, for security assurance levels 2 and 3, the Mobile Device Manufacturer is required to provide a suitable device and where appropriate (as determined by the Mobile Device Manufacturer and the MSTL), test tools.

In addition, the Mobile Device Manufacturer is required to provide configuration guidance and a description of how to perform tests which may need to be performed using debug or engineering devices with special (and sometimes non-public) tools.

5.1 Cryptographic Functionality Testing

The security functional requirements of the Protection Profile belonging to the Common Criteria FCS family shall be tested against well-known implementations for the validation of their conformity with the standards specified in the corresponding security functionality requirements.

The well-known implementation will be used in the corresponding testing tool and validation methodology. As per the ISO/IEC 17025 [3] requirements, it will be the MSTL's responsibility to validate the crypto testing methods and supporting tools.

5.1.1 Accepted Algorithms

Accepted algorithms and schemes are those that are open by design and meet the ISO criteria for approving an algorithm as an ISO standard. i.e:

- Open to the public.

- At least 3 years since publication.
- Has undergone peer review (that is publicly available).

Guidance on what algorithms would be acceptable, including in some cases how they can be tested, can be found in the following (not exhaustive or exclusive):

- NIST ACVP Protocol [10].
- SOGIS Crypto WG Agreed Cryptographic Mechanisms [11].
- ISO/IEC 18033-1:2021 [12].

5.1.2 Cryptographic Validation

There are two methods for verifying the cryptographic algorithms, directly during the evaluation or by Mobile Device Manufacturer attestation that they have already been evaluated outside of the MDSCert Scheme. These scenarios are described in more detail below.

In all cases, the MSTL shall ensure that the security functional requirements, algorithms, modes, key information and tested platforms are appropriate for the security claims being made.

For direct testing, the following scenarios are acceptable:

1. Test case study developed by the evaluator. The case study may either be entirely executed by the MSTL in an accessible instantiation of the crypto functions in the device, or be executed by the Mobile Device Manufacturer using the methodology of the MSTL and witnessed by the tester. The testing method shall be specified in the activity report.
2. Manufacturer testing attestation. The testing of the cryptographic algorithm has been performed entirely by the Mobile Device Manufacturer using their methods and tools. The Mobile Device Manufacturer provides an attestation statement about how the testing was performed. The testing method and attestation statement shall be specified in the activity report.

For attestation, the following scenarios are acceptable:

1. Certificates of cryptographic functions from well-established schemes with public results available of the algorithm, Random Number Generator or key establishment scheme tests. The existence of these certification schemes is not very common but some do exist, such as CAVP at NIST.

   In this case, publicly available information shall be enough to confirm that the certificate covers the security functional requirements (key length, modes, etc. as well as the platform on which the testing has been performed for the certification). If the platform on which the algorithm has been tested was not the same as for the device's certification, the original certificate and the operational scenario will be analysed case by case and the MSTL shall provide the MSCB with the rationale of the decision made.

2. Attestation that the cryptographic function has been tested as part of a separate certification by a MSTL participating in the MDSCert scheme. The algorithm testing may have been performed by the same or a different laboratory.

   When the original testing and the current evaluation are performed by the same laboratory, the original test results can be re-used. The MSTL shall provide the MSCB with information about the original testing (platform information) and the certification.

   When the original testing was performed by a separate lab as part of an MDSCert Mobile Device Evaluation, the Mobile Device Manufacturer shall provide evidence about the original testing (platform information) and the certification it was included in along with information about the lab that undertook the testing. The MSTL shall provide the MSCB with this attestation information along with the claim from the Mobile Device Manufacturer and where possible, an attestation statement from the original lab should be included as part of the report.

   When the original testing was performed by a separate lab outside of an MDSCert Mobile Device Evaluation, the Mobile Device Manufacturer shall provide evidence about the original testing (platform information) and the certification it was included in along with the lab information. The MSTL shall provide the MSCB with this attestation information along with the claim from the Mobile Device Manufacturer and the public report containing the original testing. If the original lab is able to provide an attestation statement, this follows as if the testing was performed within the MDSCert Scheme.

   Information/evidence to be provided by the Mobile Device Manufacturer to the MSTL: proof of commonality of the tested module and the claimed module (for example source code checksum or model of the component in use showing the tested algorithm is the same as the one in the platform under evaluation).

3. Attestation that the cryptographic function has been tested and is in a common, public component (such as a library included in the main OS) and the Mobile Device Manufacturer has not performed the evaluation directly.

   As the claim for certification is from an external source and not the Mobile Device Manufacturer, the Mobile Device Manufacturer shall only be able to use publicly available certificates from the original certification.

   Information/evidence to be provided by the Mobile Device Manufacturer to the MSTL: proof of commonality of the tested module and the claimed module (for example version number and common processor). The MSCB makes the final determination about whether the commonality is sufficient from attestation.

5.1.3 Biometric functionality testing

For the biometric mechanisms testing, the following scenarios are acceptable:

1. Manufacturer attestation or an external evaluation report demonstrating that the biometric mechanisms have been tested in meeting the FAR and FRR values indicated in the security target.

   Mobile Device Manufacturer attestation shall provide evidence of the following:

- Test procedures followed for the biometric modality.
- Number of test subjects (can be a range).
- Breakdown of gender, age, skin tone/ethnicity of the test subjects (can be listed as target percentages/ranges).
- Number of samples per test subject (number attempted, not how many are acceptable vs. failed).
- Calculations for offline testing and values used to determine success (for example incorrect matches below a threshold show having met the target FAR).

2. Test case study developed by the evaluator.

5.2 Functional Testing Verdict

A PASS verdict will be awarded if the supporting evidence provided by the Mobile Device Manufacturer allows the MSTL to assess if the objectives and security requirements have been met.

An INCONCLUSIVE verdict may be assigned for intermediate partial reports to inform the Mobile Device Manufacturer that the information provided is insufficient to meet the objectives. See section 3 for more information about remediation.

A FAIL verdict will be awarded if the supporting evidence provided by the Mobile Device Manufacturer causes the MSTL to conclude that the objectives and security requirements have not been met.

Only [PASS/FAIL] verdicts will be acceptable for the final Functional Testing Report.

5.3 Functional Testing Reports

The Evaluator shall prepare a functional technical report with a summary of the results of the testing. The report structure is defined in Evaluation output (reporting).

6 Vulnerability Analysis and Penetration Testing

While vulnerability analysis is inherently a subjective activity, a common methodology of analysis can be defined and some measure of objectivity and repeatability (or at least comparability) can be imposed on the vulnerability analysis process. To achieve such objectivity and repeatability, it is important that the Evaluator follows a set of well-defined activities and documents their findings so others can follow their arguments and come to the same conclusions as the Evaluator. While this does not guarantee that different evaluation facilities will identify the same type of vulnerabilities or come to the same conclusions, the approach defines the minimum level of analysis and the scope of that analysis and provides the MSCB(s) with a measure of assurance that the minimum level of analysis is being performed by the MSTL's evaluation facilities.

The Mobile Device Manufacturer shall ensure the MSTL has the necessary manufacturer specific tools, documentation and procedures for testing.

The Evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the Mobile Device that is the Target of Evaluation. The Evaluator shall identify and document vulnerabilities using the software and hardware information provided by the Mobile Device Manufacturer.

The Evaluator shall perform an independent vulnerability analysis of the mobile device using the available information to identify potential vulnerabilities. The vulnerability analysis shall be based on the scope defined in the ETSI TS 103 732 series [2] .

The Evaluator shall conduct independent penetration testing, based on the potential vulnerabilities identified during the independent vulnerability analysis, to determine that the mobile device is resistant to attacks performed by an attacker possessing Basic Attack Potential as defined in the Common Criteria [6]. In some cases, multiple individual vulnerabilities may be chained together to successfully attack a mobile device. Such attacks shall also be considered and rated for their attack potential. These cases shall be rationalized and highlighted in the final Vulnerability Analysis and Penetration Testing Report.

6.1 Sources of Vulnerability Information

Vulnerabilities are categorized into three “types” depending on from where they are derived, which include the following:

1. Derived from public sources that are directly applicable to the mobile device or its identified components (Type 1 Hypothesis);
2. Derived from information available to the Evaluators; this includes the evidence provided by the Mobile Device Manufacturer (Type 2 Hypothesis); and
3. Derived from the use of testing tools (e.g., nmap, fuzz testers) (Type 3 Hypothesis).

6.1.1 Type 1 Hypotheses – Public Vulnerability Based

The Evaluators shall perform a search on the sources listed below to determine a list of potential vulnerability hypotheses that are specific to the mobile device and its components. Any duplicates – either in a specific entry, or in the vulnerability hypothesis that is generated from an entry from the same or a different source – can be noted and removed from consideration by the evaluation team.

The search criteria to be used when searching the sources shall include:

- Generic terms describing one or more security functions implemented by the mobile device.
- Any protocols supported by the mobile device (these will include at least one of the remote communications protocols (IPsec, TLS, SSH)).
- The mobile device name (including appropriate model information as appropriate).
- The mobile device specific components (e.g. cryptographic libraries, underlying OS version).

As part of Type 1 vulnerability hypothesis generation for the specific components of the device, the Evaluator shall also search the component manufacturer’s websites to determine if vulnerability hypotheses can be generated on this basis (if security patches have been released for the version of the component being evaluated, the subject of those patches may form the basis for a vulnerability hypothesis).

The evaluator should use public sources of vulnerabilities to perform this activity, such as:

- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
- Common Vulnerabilities and Exposures: https://www.cve.org/
- CVEdetails.com: https://www.cvedetails.com/vulnerability-search.php
- US-CERT: http://www.kb.cert.org/vuls/html/search
- Tenable Network Security: http://nessus.org/plugins/index.php?view=search
- Tipping Point Zero Day Initiative: http://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

6.1.2 Type 2 Hypotheses – Evaluation Team Generated

The Evaluators shall formulate vulnerability hypothesis based on information presented during the Evaluation (through mobile device documentation and user guides, etc.) and mobile device behaviour during the functional testing activities. The Evaluator is also free to formulate vulnerabilities that are based on material that is not part of the baseline evidence (e.g., information gained from an Internet mailing list, or reading interface documentation on interfaces not included in the set provided by the Mobile Device Manufacturer), although such activities have the potential to vary significantly based upon the Mobile Device and the MSTL evaluation facility performing the analysis.

6.1.3 Type 3 Hypotheses – Tool Generated

The Evaluator shall perform the following activities to generate hypotheses:

- Port scanning.
- Vulnerability scanning by the use of vulnerability scanners.
- Robustness and fuzz testing.

6.2 Vulnerability Analysis Process

As vulnerability hypotheses are generated from the activities described above, the evaluation team will assess them; that is, attempt to prove, disprove, or determine the non-applicability of each hypothesis.

The Evaluator will refine each vulnerability hypothesis for the Mobile Device and will attempt to disprove it using the information provided by the Mobile Device Manufacturer or through penetration testing. For the latter, the Evaluator shall, for each hypothesized vulnerability, build a list of tests (attacks) to be performed to prove or disprove the presence of the vulnerability.

During this process, the Evaluator is free to interact with the Mobile Device Manufacturer to determine if the vulnerability exists, including requests to the Mobile Device Manufacturer for additional evidence (e.g., detailed design information, consultation with engineering staff, etc.). Should the Mobile Device Manufacturer object to the information being requested as not being compatible with the overall level of the evaluation activity and cannot otherwise provide evidence that the vulnerability is disproved, the Evaluator prepares an appropriate set of materials as follows:

- the source documents used in formulating the hypothesis, and why it represents a potential compromise against a specific mobile device function;

- an argument why the vulnerability hypothesis could not be proven or disproved by the evidence provided;
- the type of information required to investigate the vulnerability hypothesis further.

If the vulnerability has not been acknowledged by the Mobile Device Manufacturer, the Evaluator shall perform all associated defined tests that fall within the scope of the attack potential to prove or disprove the presence of the vulnerability (penetration testing activity). The tests that do not fall within the scope shall not be executed.

For each hypothesis, based on the previous activities, the Evaluator will note whether the vulnerability hypothesis has been successfully disproved, has been successfully proven to have identified a vulnerability, or requires further investigation. It is important to have the results documented as outlined in the “Vulnerability Analysis and Penetration Testing Reports” section below.

If the Evaluator finds a vulnerability, the Evaluator will report these vulnerabilities to the Mobile Device Manufacturer. All reported vulnerabilities must be addressed as follows:

- If the Mobile Device Manufacturer confirms that the vulnerability exists and that it is exploitable at Basic Attack Potential, then a mitigation solution is proposed by the Mobile Device Manufacturer, and the resulting resolution is agreed by the Evaluator and noted as part of the Vulnerability Analysis and Penetration Testing Report. The Evaluator shall repeat the associated in-scope tests to ensure that the vulnerability has been successfully remediated.
- If the Mobile Device Manufacturer, the Evaluator, and the MSTL agree that the vulnerability is exploitable only above Basic Attack Potential and does not require resolution for any other reason, then it is not necessary to provide a mitigation solution, and the vulnerability is noted as a residual vulnerability in the MSTL’s internal test report.
- If the Mobile Device Manufacturer and Evaluator agree that the vulnerability is exploitable only above Basic Attack Potential, but it is deemed critical to fix because of technology-specific aspects such as typical use cases or operational environments, then a mitigation solution is proposed by the Mobile Device Manufacturer, and the resulting resolution is assessed by the Evaluator and noted as part of the Vulnerability Analysis and Penetration Testing Report.
- Disagreements between the Evaluator and the Mobile Device Manufacturer regarding questions of the existence of a vulnerability, its attack potential, or whether it should be deemed critical to fix are resolved by the MSCB. The MSCB will review the information presented by the Evaluator and the Mobile Device Manufacturer and decide on the applicability of the vulnerability.

Any testing performed by the Evaluator shall be documented in the Vulnerability Analysis and Penetration Testing Report.

6.2.1 Attack POTENTIAL calculation

The MDSCert Scheme methodology for vulnerability analysis focuses on the exploitation phase of an attack, which corresponds to achieving the attack on another instance of the device (“not open”) using the analysis and techniques defined in the identification part of an

attack. The MDSCert Scheme methodology does not consider the creation of attacks as part of the scoring.

Attack path exploitation analysis and tests are mapped to relevant factors: elapsed time, expertise, knowledge of the Mobile Device that is the Target of Evaluation, access to the Mobile Device and equipment needed to carry out an attack.

Both remote and physical attacks are in scope. Attacks from a local network are considered to be remote attacks.

6.2.2 Attack Rating

The base reference for attack potential rating is the approach used in Common Criteria [6]. Basic attack potential is rated as depicted in the following rating of vulnerabilities and device resistance table:

Values	Attack potential required to exploit scenario	Device resistant to attackers with attack potential of	Vulnerability
0-9	Basic	No rating – the Device is vulnerable	Exploited
⩾ 9	Beyond basic	Basic	Residual vulnerability: The vulnerability exists but is beyond the basic attack potential.

Table 2 - Attack Rating

Attacks that have an attack potential score above 9 are considered out of scope at the time of the evaluation (“residual vulnerabilities”). Potential vulnerabilities that are at this level may be present in the Mobile Device but require more effort (as defined by the factors below) than is assessed in the MDSCert Mobile Device Evaluation. These potential “residual vulnerabilities” shall also be documented in the Vulnerability Analysis and Penetration Testing Report.

Over time, attack scores tend to decrease as knowledge of the tools increases, or new techniques are created, so a calculation that may be above ‘Basic’ during an initial Mobile Device Evaluation may become relevant in a later evaluation if the attack calculation computes a lower score based on changes over time. This is not guaranteed to happen at any specific rate and the calculations always need to be computed for each Mobile Device Evaluation to ensure the proper scope of attacks are verified.

The following factors and labels are used for the attack potential rating.

1. Elapsed Time: Time taken to identify and exploit
2. Expertise: Specialist technical expertise required
3. Knowledge of the Mobile Device
4. Window of Opportunity – (access to network/device)
5. Equipment required

Threat actors are considered that are able to perform attacks (defined as a set of activities intended to break or bypass a security function or control) that meet the following requirements for each of the factors that has been considered:

1. Regarding **Elapsed Time**, the value considered so that an attack can be executed by an attacker with a "Basic Attack Potential" is "**less than one month**". This means that the total amount of time taken by an attacker with a "Basic Attack Potential" to identify that a particular potential vulnerability may exist in the Mobile Device, to develop an attack method and to sustain effort required to mount the attack against the Mobile Device (considering the worst-case scenario) must be less than one month.
2. Regarding **Expertise**, the value considered so that an attack can be executed by an attacker with a "Basic attack potential" is "**proficient**". This means that the level of generic knowledge of the underlying principles, product type or attack methods (e.g. Internet protocols, Unix operating systems, buffer overflows) that an attacker exhibiting a "Basic Attack Potential" must possess are, at most, knowledgeable (compared to experts or proficient persons) in that they are familiar with the security behaviour of the product or system type;
3. Regarding **Knowledge of the device**, the value considered so that an attack can be executed by an attacker with a "Basic attack potential" is "**public**". This means that the specific expertise that the attacker must acquire concerning the Mobile Device to perform the attack is public information (e.g. as gained from the Internet) or can be acquired from the Mobile Device itself.
4. Regarding **Window of opportunity**, the value considered so that an attack can be executed by an attacker with a "Basic attack potential" is "**easy**". This means that the required access to the Mobile Device to identify and perform the attack is less than a day and that the number of Mobile Device samples required to perform the attack is less than ten.
5. Regarding IT hardware/software or other **equipment**, the value considered so that an attack can be executed by an attacker with a "Basic attack potential" is "**standard**". This means that the equipment required to perform the attack is standard equipment, readily available to the attacker. This equipment may be a part of the Mobile Device itself (e.g. a debugger in an operating system), or can be readily obtained (e.g. Internet downloads, protocol analyser or simple attack scripts).

The Evaluator can also consider the CVSS Base Metrics when considering exploitability of the vulnerability. Each of the criteria shall be considered as described below:

- Attack Vector – this score varies based on the level of access required to exploit a vulnerability. The value considered so that an attack can be executed by an attacker with a "Basic attack potential" is **Network (N**) or **Adjacent (A)**. This means that the potential vulnerability is required to be "remotely exploitable" or "limited at the protocol level to a logically adjacent topology" as described in Common Vulnerability Scoring System v3.1: Specification Document [7].
- Attack Complexity – this score varies based on the factors outside of the attacker's control that are required to exploit the vulnerability. The value considered so that an attack can be executed by an attacker with a "Basic attack potential" is **Low (L)**. This means that the attacker does not need any specialised access conditions to exploit

the vulnerability as described in Common Vulnerability Scoring System v3.1: Specification Document [7].

- Privileges Required – this score varies based on the privileges required for the attacker to conduct the exploit. The value considered so that an attack can be executed by an attacker with a "Basic attack potential" is **None (N)**. This means that the attacker is unauthorized prior to attack as described in Common Vulnerability Scoring System v3.1: Specification Document [7].
- User Interaction – this score varies based on whether the attacker must recruit either a willing or unwitting participant in order to complete their task. The value considered so that an attack can be executed by an attacker with a "Basic attack potential" is **None (N)**. This means that the attacker can exploit the Mobile Device without interaction from any user as described in Common Vulnerability Scoring System v3.1: Specification Document [7].

The CVSS v3.1 vector string is a text representation of a set of CVSS metrics. The Evaluators and Mobile Device Manufacturers can use the vector strings to automate the vulnerability search. According to the description above, the vector strings including the following values should be taken into account when considering exploitability of the vulnerability:

- Attack Vector (AV) – **Network (N)** or **Adjacent (A)**
- Attack Complexity (AC) – **Low (L)**
- Privileges Required (PR) – **None (N)**
- User Interaction (UI) – **None (N)**

6.3 Vulnerability Analysis Verdict

A PASS verdict will be awarded if no exploitable vulnerabilities are found by the Evaluator.

An INCONCLUSIVE verdict may be assigned for intermediate partial reports to inform the Mobile Device Manufacturer that the information provided is insufficient to meet the objectives.

A FAIL verdict will be awarded if the vulnerability analysis causes the MSTL to conclude that vulnerabilities that impact the Mobile Device exist and the objectives and security requirements have not been met.

Only [PASS/FAIL] verdicts will be acceptable for the final report.

6.4 Vulnerability Analysis and Penetration Testing Reports

The Vulnerability Analysis Vulnerability Analysis and Penetration Testing Report shall include the following information:

- An introduction describing the vulnerability analysis and penetration testing objectives and activity summaries
- A description of the vulnerability analysis and penetration testing strategy, including effort and time devoted by the MSTL
- A description of the Mobile Device that is the target of analysis and testing, test platforms, tools and environment used to perform the analysis and testing

- A description of the public vulnerability searches that were performed, to include keywords, search terms, NVD findings, descriptions of vulnerabilities that were included and those that were excluded and Evaluator analysis findings
- A description of the independent vulnerability analysis that was performed, to include analysis of identified vulnerabilities and Evaluator findings including the attack potential ratings for the identified vulnerabilities
- A description of the undertaken penetration tests to include prerequisites, procedures, expected outcomes, test results and verdicts including, for each performed penetration test:

    - Identification of the potential vulnerability the Mobile Device is being tested for
    - The Evaluator penetration testing effort, outlining the testing approach
    - Configuration of the test, including the steps followed in setting up the Mobile Device (and any required test equipment)
    - Execution test steps
    - Post-test procedures

- Conclusions to include observations on the overall analysis and testing process, test execution and level of compliance of the Mobile Device with the MDSCert security requirements, including:

    - Identification of the potential vulnerability the Mobile Device is being tested for;
    - Instructions to connect and setup all required test equipment as required to conduct the penetration test;
    - Instructions to establish all penetration test prerequisite initial conditions;
    - Instructions to stimulate the security function(s) being tested;
    - Instructions for observing the behaviour of the security function(s) being tested;
    - Descriptions of all expected results and the necessary analysis to be performed on the observed behaviour for comparison against expected results;
    - Instructions to conclude the test and establish the necessary post-test state for the Mobile Device;
    - A verdict of the test, that will be ‘PASS’ if the test does not prove the presence of the vulnerability, or ‘FAIL’ otherwise.

At the conclusion of the vulnerability analysis and penetration testing process, the Evaluator shall also report all exploitable vulnerabilities and residual vulnerabilities, detailing for each:

- Its source;
- A description;
- Whether it is exploitable in its operational environment (i.e. exploitable or residual).
- The amount of time, level of expertise, level of knowledge, level of opportunity and the equipment required to exploit the identified vulnerabilities;
- If the hypothesized vulnerability was solved during the evaluation by the vendor, how it was resolved (this includes whether the original vulnerability hypothesis was confirmed or disproved, and any analysis relating to whether a residual vulnerability is exploitable by an attacker with Basic Attack Potential);

7 Composition, Reuse and Equivalencies

Composition provides for the reuse of external certificates that are being relied upon as evidence of a Mobile Device's compliance with the MDSCert security requirements during evaluation. The concept of composition within the MDSCert Scheme provides a method to reuse components from both related MDSCert certificates as well as those achieved through external certification schemes. The following types of evaluations may be used when supporting an MDSCert evaluation, providing two "levels" of composition:

- Component evaluations, wherein a component (hardware or software) of the device, such as a secure element, is being used as part of the device. This embedded composition model assumes a component used as part of a larger component or the Mobile Device where no separation between the components exists. The composition evaluation shall consider that the certified component can influence other parts of the Mobile Device via its channels and interfaces. This is described in sections 7.2 to 7.4 below.
- Whole device evaluations, wherein a Mobile Device has been evaluated in its entirety (this could be either an earlier MDSCert evaluation or one outside the MDSCert Scheme). A whole device evaluation may be used to provide evidence of compliance for a component (such as an operating system that is the same on a previous MDSCert evaluation as on the new Mobile Device) or to show equivalence to the MDSCert requirements. In either case, the Mobile Device Manufacturer may plan to use that evaluation as evidence for the MDSCert Mobile Device Evaluation. The reuse of a whole device evaluation as equivalent is described in section 7.5 below (component reuse is described as above, but using the whole device certification as the evidence for the component).

While not mandatory, using externally certified components or Mobile Devices for MDSCert Certification is highly recommended. While some components might only partially contribute to the overall assurance level requirements for the evaluation and Certification of the Mobile Device, they are relevant for the overall security functionality to be assessed under the scheme.

Note: Generically, hardware and software components of the whole device are called components (instead of subcomponents).

The MDSCert Scheme approach to composition requires the following from MDSCert participating Mobile Device Manufacturers and Evaluators (regardless of the type of composition):

7.1 Component Identification

1. The Mobile Device Manufacturer shall provide the reference and version of the components that are certified under an external certification scheme that provides public results.
2. The Evaluator shall verify that the components identified by the Mobile Device Manufacturer as having been certified under an approved external certification scheme, are the same as those used in the Mobile Device that is the Target of Evaluation.

7.2 Component Scope

1. The Mobile Device Manufacturer shall identify which functionalities of the Mobile Device are relying on security services of the certified components.
2. The Evaluator shall verify that the security services of the certified components that are supporting the product functionality of the Mobile Device that is the Target of Evaluation, are in the scope of the component certification and are compliant with the product type specification, assessed against the MDSCert security requirements.

7.3 Component Assurance Level

1. The Mobile Device Manufacturer shall indicate the assurance level of certification of the components.
2. The Evaluator shall verify that the level of certification of the components is higher or equal to the targeted level for the Mobile Device that is the Target of Evaluation.

7.4 Component Composition

When using certified components in Mobile Devices for which MDSCert Certification is being sought, there are a number of programs which may be used to provide evidence of external certification that may fulfil the MDSCert Scheme Certification requirements. In general, the use of those programs applies to:

- Hardware components (e.g. Integrated Circuit/Component).
- Software components (e.g. OS, or cryptographic library).
- Mobile device platforms.

The appropriateness of an external certification for use or reuse as part of a MDSCert Mobile Device Evaluation depends on the component(s) and the security claims being made. The key requirement for the use of any external certification is the public availability of evaluation and certification results.

The following external certification schemes are accepted within the MDSCert Scheme Certification for the use/re-use of certified component certifications and the level specified is the minimum security assurance level that would be accepted as sufficient for each MDSCert Scheme security assurance level:

For Security Assurance Level 1:

- SESIP1.
- CC EAL1.
- NIST CMVP Level 1.
- ISO/IEC 19790 Level 1

For Security Assurance Level 2 & 3:

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

For all Security Assurance Levels:

- NIST CAVP.

These are not exhaustive and a Mobile Device Manufacturer may present results from additional external certification programs to the MSTL and the MSCB for reuse. The MSCB has the final say on whether any certification may be useful as direct evidence of compliance with the MDSCert security requirements.

Compliance for each of the MDSCert Scheme-supported security functionality claims will be verified by individual, valid certificates from relevant external certification programs.

Using externally certified components does not mean a Mobile Device is certified under the MDSCert Scheme. During the MDSCert Mobile Device Evaluation involving a Mobile Device that relies on composition (using externally certified components), the assessment effort is focussed on verifying the proper 'integration' of the various certified components rather than merely verifying the security claims already supported by external certifications.

Composition is also possible by reusing information from another MDSCert Mobile Device Evaluation. This will be treated in the same manner as an external certificate where information is used to satisfy the MSTL as to whether a compliance claim is properly met.

The most common MDSCert Scheme Certification reuse scenario is likely to be a main OS version that has already been evaluated on one device that has not been changed and is reused on another device. Other scenarios may include hardware that has been evaluated but does not have its own certificate. The MSTL shall report certificate reuse in the report to the MSCB and provide a justification as to the applicability and acceptance of the reused certificate.

7.5 Device Requirements Composition

Device Requirements composition is designed to help Mobile Device Manufacturers that are already certifying Mobile Devices under external certification programs and the security requirements defined under those programs. The ability to reuse external certification as evidence of MDSCert security requirement compliance depends on the mapping between the external certification scheme security requirements and the MDSCert security requirements. As with a component composition, the Mobile Device Manufacturer shall demonstrate compliance to all MDSCert security requirements.

To use any external certification, a mapping shall be provided as part of the Evaluation Technical Report to the MSCB to show and justify which of, and how, the MDSCert security requirements have been verified by the external certification.

Under Common Criteria, the following certifications may be usable as a basis for device composition:

- Common Criteria certification to the ETSI TS 103 732 series (based on the PP-Configurations) [2] .
- Common Criteria certification to the PP_MDF_V3.3 (or higher) [8].
- Common Criteria certification to a stand-alone Security Target.

By themselves, these Common Criteria certifications may not map completely to the set of MDSCert Scheme security requirements. Any MDSCert requirements not included in the

Common Criteria evaluation would still need to be evaluated for the Mobile Device to be certified for MDSCert.

The MSCB has final say on the applicability of any evidence from a prior evaluation and how it applies to MDSCert. Using the list of Security Assurance levels in section 7.4, a Common Criteria evaluation may be applied quickly to meet certain Security Assurance levels (for example a Common Criteria EAL2 could meet Security Assurance Level 3).

When using external certification evidence for use in the MDSCert evaluation, the questionnaire submitted by the Mobile Device Manufacturer to the MSTL shall include the certificate information along with any additional information necessary to fully respond to the MDSCert requirements where the external certificate may not completely answer the MDSCert requirement. This includes assurance activity evidence if the proposed evaluation is not EAL2 or higher for the proposed evaluation for composition.

7.6 Certificate Expiration under Composition

The reuse of certifications from external certification programs does not mean that all certificates can be accepted in all cases.

For MDSCert certification, any external certificate that is being relied upon to demonstrate compliance with the MDSCert security requirements shall have at least one year remaining before its expiration for it to be used as part of the composition.

The expiration of the composed certificate will not impact the ability to extend the certificate for the MDSCert Scheme but will preclude it from being used for any future compliance claims for MDSCert certification.

If an external certificate is expired it cannot be used to support MDSCert security compliance claims. A Mobile Device may still be able to meet the requirements of the MDSCert Scheme but the Mobile Device Manufacturer will not be able to use the certificate for that Mobile Device as part of its certification evidence.

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.