

TrustCB MDSCert Application Form

MDCert Application Process

TrustCB is a commercial certification body specialising in the certification of IT security, ICT security, cyber security and cryptographic products (and associated sites, processes and services) evaluated in accordance with international and industry standards.

THIS APPLICATION FORM IS INTENDED TO REGISTER AN IT SECURITY ASSESSMENT UNDER THE PROVISIONS OF THE MDSCert SCHEME OPERATED BY TRUSTCB.

THIS DOCUMENT SHALL BE COMPLETED, SIGNED AND SUBMITTED VIA E-MAIL TO MDSCERT@TRUSTCB.COM WITH "NEW MDSCert APPLICATION" IN THE SUBJECT LINE.

ADDITIONAL DOCUMENTS SHALL BE PROVIDED WITH THE APPLICATION, IN ACCORDANCE WITH THE SELECTED SECURITY ASSURANCE LEVEL:

- SECURITY ASSURANCE LEVEL 1: COMPLETED QUESTIONNAIRE + DEVELOPER EVIDENCES + EVALUATOR'S PASS VERDICT
- SECURITY ASSURANCE LEVEL 2 AND 3: COMPLETED QUESTIONNAIRE + SECURITY TARGET

When this Application Form has been completed (i.e., filled in completely and countersigned), and the associated Quotation from TrustCB has been accepted, they will together form the Certification Agreement.

Application Form reference:	<i>Reference provided by the Developer to identify this application document. Note – the default reference is the filename of this document</i>
-----------------------------	---

1 Introduction

This section describes the basics of both IT security assessment and eventual Certification Agreement.

1.1 Scheme

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

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

For details of the Scheme, see <https://trustcb.com/gsma/mdscert/>.

In this application form it is assumed that the role of Sponsor¹ may be fulfilled by the Developer of the TOE. Hence the term "Developer" is used in this document.

1.2 Terms and disclaimers

An IT security assessment under the MDSCERT scheme confirms that the TOE considered meets the specified security characteristics. It also confirms that the evaluation was conducted in accordance with the provisions of the Scheme and with the required competence and impartiality.

The evaluation results apply only to the specific version or identification of the TOE as defined in the Security Target.

Issuance of a certificate is not a guarantee that the TOE is free from security vulnerabilities. It does not absolve the Developer of any liability for damages resulting from the use of the TOE.

A certificate is not an endorsement or recommendation for use of the TOE by TrustCB or by any other organisation that recognises or gives effect to the certificate, and no warranty of the TOE by TrustCB or by any other organisation that recognises or gives effect to the certificate, is either expressed or implied. TrustCB's liability for loss and/or damages in the performance of the certification activities, an unlawful act or otherwise, is limited to the amount (exclusive of VAT) that the Sponsor has paid under this agreement. Claims beyond this point are limited to the amount paid out to TrustCB by its insurer. TrustCB will use its best endeavours to ensure the insurer pays out. TrustCB is in no event liable for indirect damages, consequential damages, lost profits, missed savings or damages through business interruption.

This agreement shall be governed exclusively by Dutch law. Any dispute will be submitted to the competent court in The Netherlands for the district where TrustCB has its registered office.

1.3 Rights and obligations

TrustCB will issue a certificate with unique certificate ID at the successful completion of a MDSCERT evaluation. The certificates for MDSCERT certified TOEs can be found at <https://trustcb.com/gsma/mdscert/>

The issued certificate does not include a Certification Mark for the scheme.

¹ As per TrustCB definitions found on the Certification Body website <https://trustcb.com>

1.1.1 Developer obligations

The Developer must comply with the published provisions of the MDSCERT scheme and shall make all necessary arrangements for the conduct of the evaluation. The provisions of the scheme are published on <https://trustcb.com/gsma/mdscert/>.

The developer confirms they will always fulfil the scheme requirements for certification as required by the scheme. This includes implementing relevant changes in scheme requirements (new or revised), where these have been communicated by TrustCB as impacting the developer's project.

Where necessary, due to the nature of the change in requirements, TrustCB shall identify the need for an activity to verify the implementation of the changes by the developer, and/or other actions as required by the scheme.

The Developer must make arrangements to investigate any complaints reported in relation to compliance of the TOE with the certification requirements.

The Developer is obligated to inform TrustCB of any issues or deficiencies in the TOE that could affect compliance with the certification requirements. This includes notifying TrustCB of vulnerabilities discovered in the TOE.

Upon completion of the certification, the developer must archive all evaluation evidence and samples.

The developer of the certified TOE:

- Shall not make any claim of certification while the TOE is still under evaluation.
- Shall ensure the certification status is understandable by their consumer and not misleading in any way.
- Shall ensure that any alteration to the TOE results in a new version of the TOE, that does not make any claim of being covered by a previously issued certificate

1.1.2 Obligations around Certificate usage

Where the certificate is referenced as evidence of the certification status of a TOE:

- The certificate shall be referenced in its entirety, as issued and/or published in the TrustCB website and with no form of abbreviation or modification
- All TOEs referencing the certificate as evidence of compliance to the scheme shall be manufactured or produced by the company or companies listed in the certificate and in a way that ensures their continuing compliance to the evaluated security characteristics
- Any advertising of the certified listing of a TOE
 - Shall be for the TOE version as described at the time of the certification assessment.
 - Shall only be for those security characteristics that were in the certified scope of the evaluation.
 - Shall be immediately discontinued when the TOE is no longer listed (i.e., certificate is expired, suspended, terminated or withdrawn).

1.3.1 Explanation of graphics, logos and marks used on Certificates

The following graphics, logos and marks may be found on TrustCB issued MDSCERT certificates and are explained as follows:

	Common Criteria mark, owned by TrustCB. Used on the certificate as a visual identifier for the Common Criteria Standards upon which the MDSCERT scheme requirements are based. This mark is not a certification mark. Use of this mark outside of the issued certificate is not permitted unless authorised by TrustCB. TrustCB reserves the right to take all necessary steps against any misuse of (Registered) Trademarks of TrustCB, as per trademark laws.
	Certificates issued by TrustCB include the TrustCB owned TrustCB logo. The TrustCB logo is not a certification mark. TrustCB reserves the right to take all necessary steps against any misuse of (Registered) Trademarks of TrustCB, as per trademark laws.

1.4 Confidentiality of the certification

TrustCB commits to the confidential management of all information obtained or created during the performance of the certification assessment activities related to this application.

TrustCB holds NDAs with all of its licensed labs to ensure confidentiality of an assessment, Developers are recommended to hold a separate NDAs with their selected (TrustCB Licensed) lab.

All information received during the course of the certification assessment for this scheme is considered proprietary information and regarded as confidential under the TrustCB category of *sensitive information*².

The exceptions to confidential handling are:

- information that the Developer agrees to make publicly available, or when agreed between the Developer and TrustCB, or otherwise authorised by contractual agreement. TrustCB shall inform the Developer in advance, when agreed information is to be placed in the public domain.
- If TrustCB is required by law or authorized by contractual arrangements to release confidential information, the developer shall, unless prohibited by law, be notified of the information provided.

At the conclusion of an evaluation and certification activity:

- If the TOE fails the evaluation, all parties shall maintain their commitment to ensure the confidentiality of this assessment.
- The associated intermediate results and verdicts produced during the evaluation are considered to be secret information regardless of outcome.
- The existence of a successful certification shall only be published if the Developer has consented to its publication in section 3.6 of this form.

² For definitions of confidentiality ratings used by TrustCB, see <https://trustcb.com>.

Where publication of the successful certification is requested to be withheld from publication ("unpublished"), TrustCB shall instead publish the SHA-256 hash of the issued certification documentation (Certificate + Security Target) as a secure means to enable it to be authenticated.

1.5 Costs related to certification

It is the responsibility of the Developer to choose an Evaluator³ and to negotiate the contractual conditions between them (including financial arrangements), before submitting this application.

TrustCB charges the costs for the certification process in accordance with the price list as published on the Scheme's website.

³ An Evaluator is an ISO 17025-accredited evaluation facility, licensed by TrustCB for this scheme.

2 Details of involved parties

This section identifies the various parties involved in the IT security assessment. It also describes the party-specific roles and responsibilities.

2.1 Developer

The Developer is the organisation that designs, manufactures, manages or maintains the TOE, or some of its components, that is subject to the assessment. The Developer is also the organisation that applies for an assessment to the Certification Body (CB), funds the evaluation and certification and shall be listed on the certificate as Certificate Holder.

The Developer is responsible for:

- defining the TOE (in the Security Target), which specifies the scope of the evaluation
- providing the TOE, Security Target, and all other evidence/evaluation documentation, including access to the relevant production and development environments of the evaluated TOE
- generating the Developer's evidence
- providing the IT product for testing
- technically assisting the Evaluator if needed (training, testing, and so on)
- providing any components of the intended operational environment necessary for testing the IT product that are not affordable or readily available to the Evaluator
- providing proof of Functional Testing.

Organisation name:	<i>Motorola Mobility LLC</i>
Address:	<i>222 W,Merchandise Mart Plaza, Chicago IL 60654 USA</i>
Commercial Contact:	<i>Lu Yu</i>
Technical Contact:	<i>Xianhong Li</i>
Telephone number:	
E-mail address:	<i>yulu11@motorola.com/lihx8@motorola.com</i>
Website:	<i>www.motorola.com</i>

Invoicing and payment details – please complete all fields:

Organisation name for invoicing:	<i>DEKRA TESTING AND CERTIFICATION, S.A.U.</i>
Chamber of Commerce reference: (company registration)	<i>A29507456</i>
VAT reference:	<i>ESA29507456</i>
Contact name (financial)	<i>Jorge Luis Carrera Borrego</i>
Address:	<i>Parque Tecnologico de Andalucia C/Severo Ochoa, 2 29590 Campanillas (Malaga) Spain</i>
Telephone number:	<i>(+34) 952619100</i>
E-mail address:	<i>jorgel.carrera@dekra.com</i>

2.2 Evaluator

The Evaluator performs the evaluation. It acts as a third party independent of the product Developer. It is licensed by the Certification Body and as such is bound to comply with the provisions of the Scheme.

To perform its work, the Evaluator shall have access to all information necessary to complete its evaluation according to the rules of the Scheme.

Organisation name:	DEKRA Testing and Certification SAU
--------------------	-------------------------------------

Address:	Severo Ochoa 2 29590 Málaga (Spain)
----------	--

Contact name:	Angel Montilla Muñoz
---------------	----------------------

Telephone number:	-
-------------------	---

E-mail address:	angel.montilla@dekra.com
-----------------	--------------------------

2.3 Certification Body

TrustCB acts as the CB and implements the MDSCERT scheme. Its primary role is to provide independent confirmation that evaluations were carried out properly, in accordance with the provisions of the Scheme, and that the conclusions of these assessments are well founded.

Organisation name:	TrustCB B.V.
--------------------	--------------

Address:	Van den Berghlaan 48, 2132 AT Hoofddorp, The Netherlands
----------	--

Telephone number:	+31 (0)23 737 08 00
-------------------	---------------------

E-mail address:	MDSCERT@TrustCB.com
-----------------	--

Website:	https://trustcb.com/gsma/mdscert/
----------	---

2.4 Scheme owner:

Organisation name:	TrustCB
--------------------	---------

Website:	https://trustcb.com/gsma/mdscert/
----------	---

E-mail address:	MDSCERT@TrustCB.com
-----------------	--

3 Scope of IT security assessment

Please complete all tables relevant to the application.

3.1 TOE description

The TOE is identified by the reference given below and is described in the referenced Security Target:

TOE Reference:	DCM:F-51G,Retail:M10	Version/ Identifier	[Android version 16]
Self-Assessment Reference:	Test Report for DCM:F-51G,Retail:M10	Version Date	2026/09/01
ST-Reference:	MTK D8450/A16	Version Date	2026/09/01
Additional documentation (add rows as needed)	Product Difference Description		

1.2 Type of Certification

Select one of the following:

Security Assurance Level 1: Verified Self-assessment	[YES]
Security Assurance Level 2: Functional Test + Document Review	[NO]
Security Assurance Level 3: Level 2 + Penetration test	[NO]
Maintenance of existing certificate (please complete 3.4)	[NO]

1.3 Not applicable for this scheme

This section is not applicable for this scheme.

3.2 In case of a request for maintenance of a certified TOE that does not impact the certified security claim

Existing Certificate ID:

Existing Certificate issue date:

Reason for maintenance:

3.3 Not applicable for this scheme

This section is not applicable for this scheme.

3.4 Publication of the certificate

After the evaluation is concluded successfully, the TOE will be listed as being certified on the Scheme's website. In the unlikely case that you do not wish the TOE to be listed, select "NO".

Publish Certificate upon successful certification

[YES / ~~NO~~]

3.5 Additional details or special requests relating to this certification

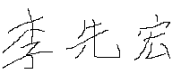
Please use this section to supply additional details relevant to the application. Note non-standard requests may incur additional certification costs.

4 Signatures

This section contains declarations to be signed by both Developer and Evaluator.

4.1 Developer

I hereby declare that I have read the terms in section 1 "Introduction" and the provisions of the MDSCERT scheme⁴, and that I commit to the responsibilities of the Developer. I also declare that all relevant contractual agreements with the Evaluator (and, where relevant, the Functional Tester) have been arranged, and that the Developer hereby requests to start the process for the evaluation and certification of the TOE identified in section 3.1 "TOE description".

Organisation name:	Motorola Mobility LLC
Signature of the person who legally represents the Evaluation Facility	
Name and title:	Xianhong Li/SW Engineer
Location:	10F, Building 1, E-Commerce Industrial Park, No. 16 Bailongjiang East Street, Jianye District, Nanjing City (Lenovo)
Date:	2026/8/24

4.2 Evaluator

I hereby declare that I have read the terms in section 1 "Introduction" and the provisions of the MDSCERT scheme, and that I commit to the responsibilities of the Evaluator. The TOE to be evaluated falls in a category for which the Evaluation Facility is licensed. I also declare that all relevant contractual agreements with the Developer (and, where relevant, the Functional Tester) have been arranged.

Organisation name:	DEKRA Testing and Certification SAU
Signature of the person who legally represents the Evaluation Facility	
Name and title:	Alvaro Ortega Chamorro (Operational Manager)
Location:	Málaga (Spain)
Date:	2026-08-24

⁴ The MDSCERT procedures, instructions, forms and all other documents can be found on the MDSCERT website (<https://trustcb.com/global-ticketing/MDSCERT/>)

Annex A: Evaluation Work Plan

The following sections of this provisional Evaluation Work Plan (EWP) must be completed and provided at the same time as this application form.

GUIDANCE FOR COMPLETION IS INCLUDED AND MARKED IN THIS MANNER (IN DARK RED). IN COMPLETED EWPs, THIS RED GUIDANCE TEXT SHOULD NOT BE PRESENT.

This EWP shall be used to estimate the certification effort and the associated certification costs. Note: any change in the evaluation scope (e.g., TOE boundary, additional evaluation meetings etc) may have contractual impact (delays, additional costs).

A.1 Scheme references

The following documents should reflect the MDSCert scheme at the time of completing the application form. **Delete unused versions/documents and update references as needed.**

TrustCB Scheme Procedure for MDSCERT*	[TrustCB_MDSCERT]	Version 1.0
TrustCB Shared Scheme Procedures *	[TrustCB_SCHEME]	Version 2.4
ETSI TS 103 732-1 - CYBER; Consumer Mobile Device; Part 1: Base Protection Profile	[PP-1]	Version 2.1.2
ETSI TS 103 732-2 - CYBER; Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module	[PP-2]	Version 1.1.2
Common Criteria for Information Technology Security Evaluation	[CC]	CC:v3.1 r5 or CC:2022 r1
Common Methodology for Information Technology Security Evaluation, Evaluation Methodology	[CEM]	CC:v3.1 r5 or CC:2022 r1

* Available to download from [TrustCB.com](https://trustcb.com)

A.2 Project communication

To establish clear communication channels, it is necessary to specify the point(s) of contact for both Developer and Evaluator.

After approval of the application, TrustCB B.V. shall inform all parties of the contact details for the assigned Certifier.

Communication of a technical nature shall be between the contacts listed in the following table and the assigned certifier(s) according to the rules specified in [MDSCERT].

Electronic versions of evaluation evidence, deliverables and reports shall be encrypted by PGP and require an exchange of public keys. The commercial certifier keys and MDSCERT key can be found on the Scheme's website, whereas the public keys of the point of contacts for both Developer and Evaluator need to be exchanged preferably with the submission of this application form.

Organisation Name	Contact	Role	E-mail
[Name of Developer]	[Xianhong Li]	SW Engineer	lixh8@motorola.com
[Name of Evaluator]	Juan Manuel Martinez Hernandez	Project Manager	juanmanuel.martinez@dekra.com
	Angel Montilla Muñoz	Lead Evaluator	angel.montilla@dekra.com
TrustCB	[Alireza Rohani]	Scheme Lead	MDSCERT@trustcb.com

A.3 Evaluation approach

(for Security Assurance Level 2 and higher)

Background

THIS SECTION SHALL DESCRIBE THE EVALUATION APPROACH EXPLAINING THE BACKGROUND, ANY RELATIONS OR DEPENDENCIES WITH OTHER EVALUATIONS, REUSE OF EVALUATION RESULTS, AND WHETHER CONSULTANCY OR OTHER ACTIVITIES (E.G., PRE-CODE REVIEWS) TOOK PLACE. IN CASE OF MAINTENANCE, PLEASE (BRIEFLY) EXPLAIN HERE THE MAJOR OR MINOR CHANGES APPLIED TO THE TOE.

Evaluation

WHAT IS THE FUNCTIONAL TESTING CERTIFICATE NUMBER (OR INTENDED DELIVERY DATE)?

Evaluation milestones

THIS SECTION SHALL DESCRIBE THE EVALUATION MILESTONES AS FORMAL EVALUATION DELIVERY MOMENTS.

Security Target (ST) Evaluation

Deliverables:	Security Target (ST)	<Delivery Date>
	ST Evaluation Report (chapter in ETR)	<Delivery Date>
Evaluation details:	ANY DEVIATIONS, REUSE OR OTHER RELEVANT INFORMATION SHALL BE DESCRIBED HERE	

Test Plan Review

Deliverables:	Evaluator Test Plan	<Delivery Date>
	ANY ADDITIONAL DELIVERABLES TO BE PROVIDED (E.G. DETAILS OF VULNERABILITY ANALYSIS PERFORMED)	<Delivery Date>
Evaluation details:	ANY DEVIATIONS, REUSE OR OTHER RELEVANT INFORMATION SHALL BE DESCRIBED HERE	

Final Evaluation Reporting

Deliverables:	Evaluation Technical Report (ETR)	<Delivery Date>
Evaluation details:	ANY DEVIATIONS, REUSE OR OTHER RELEVANT INFORMATION SHALL BE DESCRIBED HERE	