Mobile Device Security Certification Scheme – GSMA Security Requirements

Version 1.0

27 January 2025

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 is complementary to the GSMA defined Mobile Device Security Certification (MDSCert) Scheme, of which there is an overview in FS.53 - MDSCert Scheme Overview

[1]	GSMA PRD FS.53	MDSCert Scheme Overview.

.

A MDSCert Scheme requires mobile devices submitted for certification to meet security requirements as defined in the ETSI Consumer Mobile Device Protection Profile (TS 103 732) series

[2]	ETSI TS 103 732 et al	"Consumer Mobile Device Protection Profile and related documents", ETSI TS 103 732 defined by ETSI: ETSI TS 103 932-1 - V1.1.2 - CYBER; Consumer Mobile Devices Base PP-Configuration; Part 1: CMD and Biometric Verification ETSI TS 103 732-1 - V2.1.2 - CYBER; Consumer Mobile Device; Part 1: Base Protection Profile ETSI TS 103 732-2 - V1.1.2 - CYBER; Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module ETSI TS 103 732-4 – V1.1.1 – CYBER; Consumer Mobile Device; Part 4: Preloaded Applications Protection Profile Module ETSI TS 103 732-5 – V1.1.1 – Cyber Security (CYBER); Consumer Mobile Device; Part 5: Bootloader & Root of Trust Protection Profile Module

. The modified and new requirements proposed in Section 3 of this document may additionally be considered by a MDSCert scheme for inclusion as part of the security requirements against which mobile devices are assessed and certified.

1.1 Scope

The present document defines technical (functional) and non-technical (assurance) requirements identified by GSMA that could be part of a MDSCert scheme. The requirements used by a MDSCert Scheme are those defined in the latest version of ETSI TS 103 732 series

[3]	ETSI TS 103 732 et al	"Consumer Mobile Device Protection Profile and related documents", ETSI TS 103 732 defined by ETSI: ETSI TS 103 932-1 - V1.1.2 - CYBER; Consumer Mobile Devices Base PP-Configuration; Part 1: CMD and Biometric Verification ETSI TS 103 732-1 - V2.1.2 - CYBER; Consumer Mobile Device; Part 1: Base Protection Profile ETSI TS 103 732-2 - V1.1.2 - CYBER; Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module ETSI TS 103 732-4 – V1.1.1 – CYBER; Consumer Mobile Device; Part 4: Preloaded Applications Protection Profile Module ETSI TS 103 732-5 – V1.1.1 – Cyber Security (CYBER); Consumer Mobile Device; Part 5: Bootloader & Root of Trust Protection Profile Module

as detailed in Section 2. Additionally, Section 3 of the present document identifies potential gaps in security Functional and Assessment requirements, respectively, that are expected to

be addressed in future versions of ETSI TS 103 732 series: Additional requirements proposed in informative sections of this document may be considered by the Mobile Device Manufacturer to be certified under a MDSCert scheme, as mentioned in Section 3.

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	Description
Consumer Mobile Device Protection Profile	Specification written by ETSI (TS 103 732 series [4] ETSI TS 103 732 et al "Consumer Mobile Device Protection Profile and related do TS 103 732 defined by ETSI: ETSI TS 103 932-1 - V1.1.2 - CYBER; Consumer Mobile D Configuration; Part 1: CMD and Biometric Verification ETSI TS 103 732-1 - V2.1.2 - CYBER; Consumer Mobile D Base Protection Profile ETSI TS 103 732-2 - V1.1.2 - CYBER; Consumer Mobile D Biometric Authentication Protection Profile Module ETSI TS 103 732-4 – V1.1.1 – CYBER; Consumer Mobile I Preloaded Applications Protection Profile Module ETSI TS 103 732-5 – V1.1.1 – Cyber Security (CYBER); C Device; Part 5: Bootloader & Root of Trust Protection Profil) containing the security requirements for a security evaluation of consumer mobile devices.
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 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.

1.4 Abbreviations

Term	Description
CM	Configuration Management
eSE	Embedded Secure Element
ETSI	European Telecommunications Standards Institute
FCS	Functional class Cryptographic Support
FDP	Functional class user Data Protection
FIA	Functional class Identification and Authentication

Term	Description
FPR	Functional class Privacy
FPT	Functional class Protection of the TSF
GSMA	GSM Association
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
MDSCert	Mobile Device Security Certification Scheme
OS	Operating System
OTA	Over-the-Air
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SPU	Secure Processing Unit
TEE	Trusted Execution Environment
TOE	Target of Evaluation
TSF	TOE Security Functionality

1.5 References

Ref	Doc Number	Title
[5]	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
[6]	ETSI TS 103 732 et al	“Consumer Mobile Device Protection Profile and related documents”, ETSI TS 103 732 defined by ETSI: ETSI TS 103 932-1 - V1.1.2 - CYBER; Consumer Mobile Devices Base PP-Configuration; Part 1: CMD and Biometric Verification ETSI TS 103 732-1 - V2.1.2 - CYBER; Consumer Mobile Device; Part 1: Base Protection Profile ETSI TS 103 732-2 - V1.1.2 - CYBER; Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module ETSI TS 103 732-4 – V1.1.1 – CYBER; Consumer Mobile Device; Part 4: Preloaded Applications Protection Profile Module ETSI TS 103 732-5 – V1.1.1 – Cyber Security (CYBER); Consumer Mobile Device; Part 5: Bootloader & Root of Trust Protection Profile Module
[7]	GSMA PRD FS.53	MDSCert Scheme Overview.
[8]	GSMA PRD FS.54	MDSCert Scheme Test Laboratory Accreditation.
[9]	GSMA PRD FS.55	MDSCert Scheme Product Evaluation Methodology.

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

[10]	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 GSMA MDSCert Security Requirements

The security requirements in the present document define technical (functional) and non-technical (assurance) requirements identified by GSMA as part of a MDSCert scheme.

The minimum mandatory security requirements for a GSMA MDSCert scheme are defined as the following documents in the ETSI TS 103 732 series [2]:

- ETSI TS 103 932-1 - V1.1.2 - CYBER; Consumer Mobile Devices Base PP-Configuration; Part 1: CMD and Biometric Verification
- ETSI TS 103 732-1 - V2.1.2 - CYBER; Consumer Mobile Device; Part 1: Base Protection Profile
- ETSI TS 103 732-2 - V1.1.2 - CYBER; Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module
- ETSI TS 103 732-4 – V1.1.1 – CYBER; Consumer Mobile Device; Part 4: Preloaded Applications Protection Profile Module
- ETSI TS 103 732-5 – V1.1.1 – Cyber Security (CYBER); Consumer Mobile Device; Part 5: Bootloader & Root of Trust Protection Profile Module

3 GSMA Identified Security Requirements Gap

The GSMA DSG has identified a number of areas where the ETSI TS 103 732 series

[11]	ETSI TS 103 732 et al	“Consumer Mobile Device Protection Profile and related documents”, ETSI TS 103 732 defined by ETSI: ETSI TS 103 932-1 - V1.1.2 - CYBER; Consumer Mobile Devices Base PP-Configuration; Part 1: CMD and Biometric Verification ETSI TS 103 732-1 - V2.1.2 - CYBER; Consumer Mobile Device; Part 1: Base Protection Profile ETSI TS 103 732-2 - V1.1.2 - CYBER; Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module ETSI TS 103 732-4 – V1.1.1 – CYBER; Consumer Mobile Device; Part 4: Preloaded Applications Protection Profile Module ETSI TS 103 732-5 – V1.1.1 – Cyber Security (CYBER); Consumer Mobile Device; Part 5: Bootloader & Root of Trust Protection Profile Module

may not provide sufficient coverage or clarity for security requirements that are considered important to GSMA. These gaps exist due to various regulations where the requirements are not traditionally addressed using Common Criteria methodology. Additionally, though many of these security requirements are implicitly expected by the ETSI TS 103 732 series

[12]	ETSI TS 103 732 et al	"Consumer Mobile Device Protection Profile and related documents", ETSI TS 103 732 defined by ETSI: ETSI TS 103 932-1 - V1.1.2 - CYBER; Consumer Mobile Devices Base PP-Configuration; Part 1: CMD and Biometric Verification ETSI TS 103 732-1 - V2.1.2 - CYBER; Consumer Mobile Device; Part 1: Base Protection Profile ETSI TS 103 732-2 - V1.1.2 - CYBER; Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module ETSI TS 103 732-4 – V1.1.1 – CYBER; Consumer Mobile Device; Part 4: Preloaded Applications Protection Profile Module ETSI TS 103 732-5 – V1.1.1 – Cyber Security (CYBER); Consumer Mobile Device; Part 5: Bootloader & Root of Trust Protection Profile Module

, more explicit security requirements would avoid possible misinterpretations and provide greater clarity for MDSCert scheme participants. These gaps have been communicated to ETSI TC CYBER for consideration.

A MDSCert scheme shall use the security requirements defined in section 2 for its evaluation. In addition, a MDSCert scheme may also determine that its evaluation could include the additional security requirements that are described in this section of the present document. If such security requirements are included, the certification report shall make it clear which GSMA security requirements were assessed in addition to those from the ETSI TS 103 732 series

[13]	ETSI TS 103 732 et al	"Consumer Mobile Device Protection Profile and related documents", ETSI TS 103 732 defined by ETSI: ETSI TS 103 932-1 - V1.1.2 - CYBER; Consumer Mobile Devices Base PP-Configuration; Part 1: CMD and Biometric Verification ETSI TS 103 732-1 - V2.1.2 - CYBER; Consumer Mobile Device; Part 1: Base Protection Profile ETSI TS 103 732-2 - V1.1.2 - CYBER; Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module ETSI TS 103 732-4 – V1.1.1 – CYBER; Consumer Mobile Device; Part 4: Preloaded Applications Protection Profile Module ETSI TS 103 732-5 – V1.1.1 – Cyber Security (CYBER); Consumer Mobile Device; Part 5: Bootloader & Root of Trust Protection Profile Module

.

3.1 Security Functional Requirement Gaps (Informative)

The proposed security functional requirements are based on the requirements from the ETSI TS 103 732 series

[14]	ETSI TS 103 732 et al	"Consumer Mobile Device Protection Profile and related documents", ETSI TS 103 732 defined by ETSI: ETSI TS 103 932-1 - V1.1.2 - CYBER; Consumer Mobile Devices Base PP-Configuration; Part 1: CMD and Biometric Verification ETSI TS 103 732-1 - V2.1.2 - CYBER; Consumer Mobile Device; Part 1: Base Protection Profile

		ETSI TS 103 732-2 - V1.1.2 - CYBER; Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module ETSI TS 103 732-4 – V1.1.1 – CYBER; Consumer Mobile Device; Part 4: Preloaded Applications Protection Profile Module ETSI TS 103 732-5 – V1.1.1 – Cyber Security (CYBER); Consumer Mobile Device; Part 5: Bootloader & Root of Trust Protection Profile Module

and introduce modifications to cover the gaps identified by GSMA DSG. The formatting and conventions of requirements text, both in GSMA proposed modified requirements in sections 3.1.1 and GSMA proposed new requirements in section 3.1.2, are defined in ETSI TS 103 732-1 section 8.2

[15]	ETSI TS 103 732 et al	"Consumer Mobile Device Protection Profile and related documents", ETSI TS 103 732 defined by ETSI: ETSI TS 103 932-1 - V1.1.2 - CYBER; Consumer Mobile Devices Base PP-Configuration; Part 1: CMD and Biometric Verification ETSI TS 103 732-1 - V2.1.2 - CYBER; Consumer Mobile Device; Part 1: Base Protection Profile ETSI TS 103 732-2 - V1.1.2 - CYBER; Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module ETSI TS 103 732-4 – V1.1.1 – CYBER; Consumer Mobile Device; Part 4: Preloaded Applications Protection Profile Module ETSI TS 103 732-5 – V1.1.1 – Cyber Security (CYBER); Consumer Mobile Device; Part 5: Bootloader & Root of Trust Protection Profile Module

, unless otherwise specified in the present document.

3.1.1 ETSI TS 103 732-1 GSMA Modified Security Functional Requirements

The following security functional requirements (SFRs) from the Base-Protection Profile (PP) are proposed to be modified for a MDSCert Scheme. The modifications to the SFR as it exists in the PP are highlighted in yellow.

3.1.1.1 Class: User Data Protection (FDP)

3.1.1.1.1 FDP_UPF_EXT.1/SSW_Update Update check frequency

FDP_UPF_EXT.1.1/SSW_Update The TSF shall be able to check for a [SYSTEM SOFTWARE] update package every [assignment: ~~*interval period*~~ ***an interval of no more than 1 month***] and provide a notification to the user when an update is available.

3.1.2 New Security Functional Requirements

The following SFRs are new and not currently included in the ETSI TS 103 732 series

[16]	ETSI TS 103 732 et al	"Consumer Mobile Device Protection Profile and related documents", ETSI TS 103 732 defined by ETSI: ETSI TS 103 932-1 - V1.1.2 - CYBER; Consumer Mobile Devices Base PP-Configuration; Part 1: CMD and Biometric Verification ETSI TS 103 732-1 - V2.1.2 - CYBER; Consumer Mobile Device; Part 1: Base Protection Profile ETSI TS 103 732-2 - V1.1.2 - CYBER; Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module

		ETSI TS 103 732-4 – V1.1.1 – CYBER; Consumer Mobile Device; Part 4: Preloaded Applications Protection Profile Module ETSI TS 103 732-5 – V1.1.1 – Cyber Security (CYBER); Consumer Mobile Device; Part 5: Bootloader & Root of Trust Protection Profile Module

.

3.1.2.1 Class: Cryptographic Support (FCS)

The device shall protect keys from the main operating system (OS) and store them in a location that is tied to hardware on the device that cannot be directly accessed.

3.1.2.1.1 FCS_STG_EXT.1 Hardware-supported Cryptographic Key Storage

FCS_STG_EXT.1.1 The Target of Evaluation Security Functionality (TSF) shall provide [selection: *hardware-based, hardware-isolated*] secure cryptographic key storage.

NOTE: Hardware-based => Trusted Execution Environment (TEE) or similar

Hardware isolated => Embedded Secure Element (eSE), Secure Processing Unit (SPU) or similar

FCS_STG_EXT.1.2 The TSF shall utilize the provided secure cryptographic key storage for protecting the key hierarchy.

3.1.2.1.1.1 Evaluation Activity

The evaluator shall review the documentation provided by the developer and verify it describes how the key hierarchy is securely stored and accessed in the TOE. The description shall include how the keys in the key hierarchy are stored utilizing the specified secure cryptographic key storage. The description shall specify how this protection is tied to the hardware and any protections against direct access (this may be demonstrated as part of other requirements).

3.1.2.2 Class: Identification and Authentication (FIA)

The biometric mechanism shall provide sufficient protection against spoof (presentation attack) attempts. This is measured by the Spoof Acceptance Rate of the sensor.

3.1.2.2.1 FIA_SAR.1 Biometric Spoof Acceptance Rate

FIA_SAR.1.1 The TSF shall provide a biometric verification mechanism with the Spoof Acceptance Rate [selection:

- *BELOW 7%*
- *BETWEEN 7-20%*
- *ABOVE 20%].*

3.1.2.2.1.1 Evaluation Activity

The evaluator shall review the documentation about testing for spoof acceptance (presentation attack) to verify the presented Spoof Acceptance Rate. The documentation shall include information about the test environment, users, samples and presentation methodology. The documentation shall provide sufficient information about the spoof

acceptance evaluation process to understand how the testing is performed and that it is adequate.

3.1.2.3 Class: Privacy (FPR)

Over-the-Air (OTA) clients shall follow the same requirements as other preloaded apps and not have permissions which grant access to user data or potential malware.

3.1.2.3.1 FPR_ANO.2 Anonymity without soliciting information.

FPR_ANO.2.1 The TSF shall ensure that [*THE SYSTEM SOFTWARE OTA CLIENT*] is unable to determine the real user data bound to [*the TOE (HARDWARE PLATFORM)*].

NOTE: To function properly, the OTA client will have a high level of system permissions, and the OTA system may require a combination of a Device ID and a valid user account to access the OTA update. The definition of real user data encompasses user data that is associated with any of the applications or services on the device. This requirement specifies that the real user data on the device is not accessible to the OTA client regardless of the system permissions assigned to the OTA client.

FPR_ANO.2.2 The TSF shall provide [*SYSTEM SOFTWARE UPDATES*] to [*THE USER*] without soliciting any reference to the real user data.

3.1.2.3.1.1 Evaluation Activity

The evaluator shall review the documentation provided by the developer and verify that it describes the permissions assigned to the OTA client and how these prevent access to any user data. The information necessary to access the OTA system (such as the Device ID and a valid user account) to authorize the download of the update shall be specified. No other data should be accessible to the OTA client.

3.1.2.4 Class: Protection of the TSF (FPT)

The devices shall ensure that access to local services with system permissions are not accessible to the network for incoming requests. Similarly, critical functions such as AT commands shall not be available to remote control without the user being able to confirm the access request.

3.1.2.4.1 FPT_EAT_EXT.1 External Access to AT Modem Commands

FPT_EAT_EXT.1.1 The TSF shall only allow access to AT modem commands from *[selection: the user interface, user-approved external connection, user-approved remote connection, [assignment: other interfaces]*].

FPT_EAT_EXT.1.2 The TSF shall prompt for approval of AT modem commands sent to the device from outside the user interface [selection: *at the time of the connection that will send the command, for each command*].

NOTE: Each of the interfaces provides a method for user-approval. The direct user interface is implicitly approved as the device is unlocked and directly in use to enter the commands. How the user-approval is provided for any other (anything that is not the user interface) connection shall be described. If no

commands can be sent, the open assignment can be used to specify “no interfaces.”

3.1.2.4.1.1 Evaluation Activity

The evaluator shall review the documentation provided by the developer and verify that each method for submitting AT modem commands is described. Any interfaces beyond the user interface shall have a description of how the connection is established, at what point the user authorizes the connection, and how the session is terminated (such that the connection is not persistent).

3.1.2.4.2 FPT_LNW_EXT.1 Loopback Network Sockets

FPT_LNW_EXT.1.1 The TSF shall ensure that no listening network sockets to the external or loopback IP networks are associated with processes with system permissions on the device.

FPT_LNW_EXT.1.2 The TSF shall ensure that [assignment: *Network sockets and associated processes*] exposed to the external or loopback IP networks have no system permission on the device.

3.1.2.4.2.1 Evaluation Activity

The evaluator shall review the documentation provided by the developer and verify the descriptions about available Internet Protocol (IP) network sockets. The evaluator shall confirm that any IP network sockets that are available as an externally available service (e.g. accepting incoming requests that are not responses to outgoing requests) are not associated with any processes with system permissions on the device.

3.2 Security Assurance Requirement Gaps (Informative)

The Mobile Device Manufacturer shall have a process for receiving information about vulnerabilities and then provide patches for those vulnerabilities to the impacted devices. In addition, this includes a defined period and frequency of updates to the device (including both OS updates and regular security patches).

As part of this process, the Mobile Device Manufacturer will have a vulnerability disclosure program to receive information and provide patches (and document the patches publicly).

The Mobile Device Manufacturer shall document how external updates for components used in the device (such as external software packages, hardware components or other code) are incorporated into updates for the device.

The Mobile Device Manufacturer shall document how the device signing keys are managed, from the internal servers to the devices (both development and production).

3.2.1 ETSI TS 103 732-1 GSMA Modified Security Assurance Requirements

The following security assurance requirements (SARs) from the Base-PP are modified for a MDSCert Scheme. The entire SAR is not copied here, only the parts that are modified or added, with those changes highlighted in yellow.

3.2.1.1 ALC_CMC.2 Use of a CM system

ALC_CMC.2.4D The developer shall provide guidance for importing and updating external software components into the CM system.

ALC_CMC.2.4C The CM documentation shall describe the method used to identify external software components and how those components are updated.

3.2.1.2 ALC_CMS.2

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE including any external software components.

ALC_CMS.2.2E The evaluator shall confirm that for external software components, the developer shall include the source and original maintainer of the component.

3.2.1.3 ALC_DVS_EXT.1 Identification of security measures for device identifiers and keys

ALC_DVS_EXT.1.1D The developer shall produce and provide development security documentation on the generation, ~~and~~ protection and use of signing keys ~~and device unique identifiers~~.

ALC_DVS_EXT.1.2D The developer shall produce and provide development security documentation on the acquisition or generation of device unique identifiers.

ALC_DVS_EXT.1.3D The developer shall produce and provide development security documentation on the provisioning of data or keys that may be used by a Root of Trust.

ALC_DVS_EXT.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the ~~following manufacturing components:~~ keys used to sign the publicly released system software and its updates.

ALC_DVS_EXT.1.2C The development security documentation shall describe the procedures for selecting the proper signing keys used for a device and to ensure the use of the proper keys in the build process.

ALC_DVS_EXT.1.3C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the ~~following manufacturing components:~~ unique, non-modifiable identifiers (such as IMEI, attestation keys or Device Unique Keys) and how they are properly acquired/created and provisioned for each device.

ALC_DVS_EXT.1.4C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the ~~following manufacturing components:~~ data and keys provisioned to the device for a Root of Trust for the device.

3.2.1.4 ALC_FLR.3 Systematic flaw remediation

ALC_FLR.3.4D The developer shall provide public guidance related to the duration period, frequency and type of updates that will be released to support the TOE.

ALC_FLR.3.5D The developer shall provide a public vulnerability disclosure program to provide security bulletins about the flaws that have been remediated.

ALC_FLR.3.6D The developer shall establish procedures for ensuring that no known security vulnerabilities rated as High and Critical (e.g. as classified in public databases) are included in the TOE at public release.

ALC_FLR.3.12C The flaw remediation procedures documentation shall define the planned minimum duration after release of the TOE that these methods will be used to maintain the TOE.

ALC_FLR.3.13C The flaw remediation procedures documentation shall define the types of updates (such as security/maintenance or operating system) and the frequency of these updates being provided for the TOE.

ALC_FLR.3.14C The flaw remediation procedures documentation shall describe the process for publicly releasing security flaw remediation information, including the location(s) where this will be publicly available.

ALC_FLR.3.15C The flaw remediation procedures documentation shall describe the process for verifying known security flaws are not propagated into a new (not yet released) TOE.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	27 Jan 2025	First version	ISAG	Alex Leadbeater, GSMA

A.1 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.2 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 prd@gsma.com

Your comments or suggestions & questions are always welcome.