Device Anti-Theft Requirements
Version 4.0
17 July 2026

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Compliance Notice

The information contain herein is in full compliance with the GSM Association's 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 in GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1 Introduction

To date, there have been various efforts and a variety of approaches taken to address the issue of mobile device theft. Some include technical capabilities and processes implemented by mobile network operators to control device access to their networks via IMEI validation using Equipment Identity Registers (EIRs) and the sharing of blocklisted IMEIs by connecting EIRs to the GSMA's Device Registry. These solutions are outlined in section 4 and they have been in place for many years, with the solutions continuing to be improved and extended.

The issue of mobile device theft has prompted various government agencies around the world, and in the UK and USA in particular, to ask the mobile industry for assistance with trying to resolve this problem. This effort has captured the attention of the popular press and has been widely reported on to the point that the concept of a "Kill Switch" has entered the common lexicon. The Kill Switch concept and proposed legislation are considered and are summarised in Annex B.

Mindful of the fact that a range of stakeholders, including users have a role to play to combat device theft, this document describes mechanisms to assist device owners to combat and protect themselves from theft. These mechanisms include the ability to disable service to a mobile device and to restore the device to an operational state if the device is returned to its owner. In addition, various anti-theft features that are currently offered by device manufacturers, (a term used herein to include OS providers), a list of third party tools that can be used to locate lost devices and other resources device users can use to safeguard their devices and data from theft are located on the GSMA's website at: https://www.gsma.com/solutions-and-impact/technologies/security/security-advice-for-mobile-device-users/

1.1 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 RFC 2119 [3] and clarified by RFC 8174 [4], when, and only when, they appear in all capitals, as shown here.

2 Definitions, Abbreviations and Requirements Format

This section describes terms and abbreviations that are used within this document, as well as explaining how requirements are defined.

2.1 Definitions

Term	Definition
Authorised Device User	Any natural person who is authorised to use a device with the knowledge and permission of the Owner. A Device User may be the Owner or a different person (e.g. an employee, family member, or temporary borrower). Being a Device User does not, by itself, grant authority to invoke anti-theft controls (e.g. disable, wipe, or re-enable) unless such authority is explicitly granted by the Owner.

Device	A handheld cellular radio telephone that includes all of the following features: (i) utilises a mobile operating system; (ii) possesses the capability to utilise mobile software applications, access and browse the Internet, utilise text messaging, utilise digital voice service, and send and receive e-mail; (iii) has cellular network connectivity, and (iv) supports device anti-theft features. Examples are smartphones, cellular-connected wearables and cellular-connected tablet devices that meet the criteria of this definition are considered in scope. Out of scope devices are those that do not have SIM/eSIM functionality and an IMEI, those that do not include a radio cellular telephone commonly referred to as a "feature" or "messaging" phones, a laptop or a device that only limited non-cellular capabilities, such as some e-book readers.
Device Hardware	The physical components that together make a functioning mobile device including screen printed circuit board, chips, SIM card (including embedded SIMs, eSIMs or integrated SIMs), removable storage, etc.
Device Software	All software programs on the device and SIM card (including embedded SIMs, eSIMs or integrated SIMs), including applications, operating system, boot loader, boot-ROM, and firmware.
eSIM	eSIM is the top-level generic descriptor applied to the Devices and eUICCs that support Remote SIM Provisioning, as defined in GSMA PRD SGP.21 [2].
Kill Switch	A 'Kill Switch' is a way to disable crucial functions of a mobile device. It is essentially a function within the mobile equipment, so that if triggered e.g., by a message of some format that is sent to it, then the mobile will cease to operate as it is intended to and can only be reactivated or reused if the device owner authorises the reactivation of the device.
Locked[1]	The device display/keyboard/keypad does not allow access to device features and applications and is password protected. To unlock the device the correct password needs to be entered. This is a common feature on devices where the owner sets a password for the device which is required to gain access to the display, keyboard and applications. This feature is normally activated at device power up, restart, and after a period of inactivity.
Owner	The natural person or legal entity that holds title to, or contractual rights of control over, a device and may delegate administrative authority for that device. The owner may be an individual consumer, an enterprise, an institution, an MNO, or a reseller that has purchased the device directly or indirectly from the OEM. Ownership can coexist with authorised use by others; for example, an enterprise may authorise an employee to use

[1] This definition and the content in 6.19 below has been reproduced with permission from the Alliance for Telecommunications Industry Solutions (ATIS) from ATIS-0700024, *Best Practices for Obtaining Mobile Device Identifiers for Mobile Device Theft Prevention (MDTP)*. © 2015 Alliance for Telecommunications Industry Solutions (ATIS). A copy may be obtained viahttps://www.atis.org/docstore/product.aspx?id=28245.

	a device while retaining ownership for a certain period of employment, and an MNO or reseller may lease a device to an individual while retaining ownership during the lease or an initial commitment period. References in this document to actions by the owner include actions performed by an owner, authorised administrator or representative in accordance with the owner's policies, applicable law and, where required, user consent. For the purposes of this document, it is assumed that there is a single owner at any given time.
Roaming	Roaming is the ability for a mobile user to automatically make and receive telephone calls, send and receive data, or access other services while travelling outside the geographical coverage area of the home mobile network, by means of using a network of another mobile operator.

2.2 Abbreviations

Abbreviation	Definition
3G	A third generation mobile network (for example UMTS)
3GPP	3rd Generation Partnership Project
CEIR	Central Equipment Identity Register (the former name of the Device Registry)
EIR	Equipment Identity Register
eSIM	Embedded SIM
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GSMA	The GSM Association
IMEI	International Mobile Equipment Identity Note: In 5G this is referred to as the Permanent Equipment Identifier (PEI), which is an IMEI for devices capable of accessing 3GPP compliant networks.
ISP	Internet Service Provider
MNO	Mobile Network Operator
MSISDN	Mobile Station International Subscriber Directory Number (a telephone number)
OEM	Original Equipment Manufacturer
OS	Operating System
OTP	One Time Password
PLMN	Public Land Mobile Network
ROM	Read Only Memory
SEIR	Shared Equipment Identity Register – occasionally a subset of the data on the Device Registry within a group of mobile networks or a country
SIM	Subscriber Identity Module
SMS	Short Message Service (a text message)
UMTS	Universal Mobile Telecommunications System (3G)
Wi-Fi	A wireless technology based on IEEE 802.11 standards

2.3 References

Ref	Doc Number	Title
[1]	GSMA Mobile Device Theft Whitepaper	Mobile Device Theft - State of Affairs Report https://www.gsmaservices.com/wp-content/uploads/2025/02/Tackling-device-theft-high-res-FINAL-18-feb-25.pdf
[2]	SGP.21	RSP Architecture https://www.gsma.com/solutions-and-impact/technologies/esim/gsma_resources/sgp-21-architecture-specification-v2-3/
[3]	RFC 2119	"Key words for use in RFCs to Indicate Requirement Levels", S. Bradner http://www.ietf.org/rfc/rfc2119.txt
[4]	RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words https://www.rfc-editor.org/info/rfc8174
[5]	The Telegraph	Introduce kill switch to smartphones to stop theft, February 2025 https://www.telegraph.co.uk/news/2025/02/06/introduce-kill-switch-to-smartphones-to-stop-theft/
[6]	Daily Mail	Apple and Google face calls to install kill switches on mobile phones, 2025 https://www.dailymail.co.uk/news/article-14944839/Apple-Google-face-calls-install-kill-switches-mobile-phones-stolen-moped-gangs-end-resale-market.html
[7]	Mobile World Live	Nvidia stands firm on backdoor kill switch debate https://www.mobileworldlive.com/nvidia/nvidia-stands-firm-on-backdoor-kill-switch-debate/
[8]	GSMA TS.06	GSMA IMEI Allocation and Approval Guidelines https://www.gsma.com/get-involved/working-groups/gsma_resources/ts-06/
[9]	GSMA FS.31	Baseline Security Controls https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2019/03/FS.31-Baseline-Security-Controls-v7.0.docx
[10]	ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection - Information security management systems - Requirements https://www.iso.org/standard/27001
[11]	OMTP TR1	Advanced Trusted Environment: OMTP TR1 http://www.omtp.org/OMTP_Advanced_Trusted_Environment_OMTP_TR1_v1_1.pdf
[12]	3GPP TS 22.016	International Mobile station Equipment Identities (IMEI) https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=567
[13]	GSMA IMEI Security Technical Design Principles	IMEI Security Technical Design Principles: Enabling stolen mobile device blocking

		https://imeidb.gsma.com/imei/resources/documents/IMEI-Security-Technical-Design-Principles-v4.pdf
[14]	3GPP TS 22.030	Man-Machine Interface (MMI) of the User Equipment (UE) https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=570

2.4 Requirements Format

Requirements are formatted as follows: XXX-YYY-ZZZZ

Where:

XXX denotes this document: ATH (Anti-Theft),

YYY denotes the related section: e.g., LOC (Location Features),

ZZZZ denotes a four digit numbering format which increments by 10 numbers for each requirement, allowing for future updates: e.g., 0020, 0030 etc.

Normative text (i.e., the requirements) is contained within the requirements tables. The remainder of the text is considered to be non-normative and therefore informative and supporting text.

3 Scope

To move the mobile industry towards a mechanism that would allow the remote disabling of a mobile device requires a structured approach and assessment of the problem. The GSMA, as it represents over 1,000 mobile network operator and supplier companies in more than 220 countries, can facilitate exploration of solution options by defining the characteristics of features and by achieving consensus of its membership, that could lead to a consistent implementation of solutions that are widely supported by operators and device manufacturers.

This document defines a set of requirements which can be used by device manufacturers, mobile network operators, and third-party service providers, to offer a set of features to device owners and authorised device users to assist in locating lost/stolen devices and to protect the data within the device. Separately, mechanisms to combat supply chain theft are also discussed alongside consumer theft requirements, when applicable. Additionally, these requirements may be useful as a guide for governments and legislators in the formation of legislation related to mobile device theft prevention and, in some circumstances, law enforcement agencies may also find these tools useful.

The features which implement these requirements are envisioned to operate at the application level of the device software architecture, although device manufacturers may choose to embed these features in the operating system. The implementation of these features may also require support from mobile network operator infrastructure or other third party or manufacturer provided servers that are accessible to device owners and authorised device users via the Internet. Additionally, some or all of the features listed in this document, and the enablement of them, may be offered via a technical support/customer care call centre.

These requirements have the potential to set a benchmark for anti-theft features that are offered to mobile device owners and authorised device users, and at the same time leave the device manufacturers, mobile network operators, and third-party service providers free to design specific offerings in a way that best suits their devices and businesses. Thus, the ability of the industry to innovate is not being stifled whilst the objective is retained that a core set of anti-theft functionalities is defined for all devices.

The scope of work in this document is focussed on securing the owner's and authorised user's device and data using software features available on the device, within the mobile network and/or the supply chain to minimise risk and loss to all stakeholders. It is not in the scope of this document to address situations when the device hardware or IMEI integrity is compromised through tampering, disassembly/reassembly, etc. The sections in this document on 'Prevention of Unauthorised Device Re-initialisation' and 'Securing IMEI' call for continued attention to, and evolution of, foundational device hardware and software security measures within the context of an ever-shifting threat landscape.

The effectiveness and efficiency of all anti-theft features are directly linked to, and are dependent on, the strength and ability of the device to resist attacks from individuals and organisations that are engaged in the trafficking of stolen devices and who are determined in their efforts to crack or otherwise compromise the protection mechanisms. Thus, the success of this GSMA initiative to promote the development and adoption of device based anti-theft measures will rely, in part, on the capacity of the device manufacturers, and their suppliers, to deliver strong and robust implementations.

Further details on the mobile industry's previous work in this area can be found in the Mobile Device Theft – State of Affairs Report **Error! Reference source not found.**

3.1 Theft Journeys

Since the introduction of mobile devices, they have been targeted by thieves. There are multiple methods of acquisition and for the purposes of this document, two main categories will be considered.

3.1.1 End user theft

End-user mobile device theft encompasses a range of criminal activities directly targeting individuals. A device may be stolen in a locked state (e.g. pick pocketing) or in an unlocked state (e.g. phone snatching). Criminals can profit from direct hardware resale of the device and its components, data/identity theft from the device content and abuse of payment functionality.

3.1.2 Supply chain theft

Supply chain theft specifically refers to theft occurring before the device reaches an end user. It could happen during manufacturing, transportation or storage and typically happens in bulk. In most supply chain theft cases, the stolen devices have not yet been initialised by end users, so most consumer theft protection features do not apply.

4 Network Based Anti-Theft Mechanisms

Network based approaches to combat device theft are briefly outlined in this section. The mobile network operator's primary tool used to prevent the connection and use of stolen or counterfeit devices is the Equipment Identity Register (EIR), which contains a domestic blocklist and the sharing and consolidation of blocklists from multiple operators from various jurisdictions via the GSMA's Device Registry. These capabilities are used to block devices from receiving service based on the IMEI transmitted by the device to the mobile network. Some enhancements to the traditional approaches that use currently available technologies are also outlined.

4.1 Network Based Anti-Theft Solutions

Network based anti-theft measures have been in existence for many years and have been actively promoted by the GSMA. The most prevalent in use is the EIR, which is defined in the 3GPP published open standards.

Operator EIRs determine whether device access to a mobile network is allowed or blocked based on validating and checking an IMEI against lists of mobile device identifiers that are allowed or denied network access. Operators can prevent the transfer of stolen devices from one mobile network to another by sharing their individual blocklists. This has been accomplished in many countries via a local national shared EIR (SEIR). Connection to the GSMA Device Registry and use of its data in individual operator EIRs is an important and valuable resource to block stolen devices from accessing domestic and overseas mobile networks in order to reduce the cross-border trafficking of stolen devices. Operators can export their stolen lists to contribute to the content of the GSMA Device Registry and thereby facilitate the widest possible international blocking of those devices.

Network based anti-theft measures apply to any kind of device whereas some of the device-based features described below can only be supported by smartphones. Therefore, the support of all or part of the device-based requirements will depend on the type and capability of an individual device, but mobile network-based solutions can be applied to all mobile devices.

5 Mobile Device Anti-Theft Disablement (Kill Switch)

5.1 Kill Switch Background and Concerns

Periodically, the topic of a Kill Switch for mobile devices enters political parlance. Proposals in the late 1990s were for hardware disablement by remotely blowing fuses on the silicon substrate, this led to a misinterpretation of this as 'exploding phones'. The Kill Switch became a popular term in 2013 when a number of public officials and politicians, most notably the Mayors of London, San Francisco and New York, asked the mobile industry for assistance in combating mobile device theft. Device anti-theft measures, such as locking to prevent the re-enablement of devices, have been deployed by industry, as further described in the GSMA white paper **Error! Reference source not found.**. However, in 2025, there were renewed calls for kill switches from the UK's Home Secretary and the Metropolitan Police, reported in the press as "to stop moped gangs, end resale markets" and "to stop the mugging epidemic" [5] [6]. None of these statements clearly, technically, define what a kill switch is, other than a mechanism to remotely and completely disable a device.

While policy makers might prefer a centralised model for rapid broad response to theft or misuse a clear definition of what constitutes a kill switch is missing. Broadly, it implies some mechanism to remotely disable use of the essential features of a mobile device once it has been stolen or is otherwise no longer in the possession of the owner or authorised user.

A centralised mechanism built into the mobile infrastructure to disable a mobile device, is seen as a very dangerous tool that has the potential to be abused in a way that would generate a huge cybersecurity risk to the mobile industry and users. It could be used as a powerful cyber weapon. In an adjacent industry, Nvidia's Chief Security Officer stated that kill switches for its chips would be "a gift to hackers and hostile actors" [7].

Permanently disabling or "bricking" an entire device is a more severe action than disabling mobile service. It also does not provide the user, in the event of an error, with a clear recourse for remedy because they may not have an ongoing business relationship with the device manufacturer in the same way as they do with their mobile service provider. Instead, the GSMA recommends device manufacturers to provide locking and disabling functionality based on their own relationship with the device owner, via a dedicated user account, or similar.

As an alternative, the GSMA Device Security Group (DSG) originally developed this document, and continues to maintain it, for device manufacturers, mobile network operators and governments. It defines a set of features that can be invoked by a device owner or authorised user to locate, disable, and re-enable their device if it is misplaced, lost or stolen. These features can only be invoked by the owner of the device and can only be applied to the device registered to the owner. Precautions must be taken to validate and verify ownership to avoid abuse. The implementation of these capabilities and tools will be done by device manufacturers (and other industry service providers) and while the baseline protections will be similar across mobile devices, the implementation can, and is likely to, be different for each provider. This decentralisation of the disabling function down to the user level will make it difficult for any unauthorised mass disabling of mobile devices although each implementation must ensure the security of its feature against criminal acts and unauthorised triggering. Each device manufacturer is free to develop features that are specific to its products but providing similar baseline functionality across all manufacturers to assist the owners in retrieving their devices and/or safeguarding the user data is the ultimate objective of the requirements described in this document.

5.2 Device Anti-Theft Features and IMEI Blocking

The disabling feature envisioned by this document does not reduce the need for the use of network based anti-theft features. Mobile network operators will continue to use the EIR and Device Registry to block network service to blocklisted IMEIs, including dealing with fraud issues. Blocking an IMEI only stops the device from obtaining wide-area cellular service on networks that use the relevant blocklists.

IMEI blocking can prevent devices accessing mobile networks, but it does not preserve or protect the data on the device or otherwise restrict its use. Authenticated device owners and authorised device users can invoke additional services provided by manufacturers or service providers to further restrict device functionality such as by locking, locating or resetting devices. The features outlined in this document will complement the IMEI blocking service

and give owners and authorised device users additional tools to protect their data on the device and to retrieve it in a way that IMEI blocking cannot.

In the following section, requirements for theft prevention features are provided and all the above common technical requirements are addressed.

6 Requirements for Anti-theft Device Features

The basic model behind these requirements envisages the involvement of the owner or authorised device user and the mobile network operator as the two actors involved in the execution of the disabling feature that renders essential functions on a device unusable to unauthorised persons, other than emergency service access, as described in section 6.

The first working scenario is where the owner or authorised device user, having become aware their device is missing (be it stolen or misplaced), decides to contact their MNO to seek assistance with the necessary steps to disable the device. The second scenario is where the owner or authorised user has direct access to a disabling tool via a website interface or application available on an alternate mobile device.

6.1 Disabled Device Functionalities

A disabled device is unable to connect to a MNO, as the device is rejected during the initial network handshake. This effectively disables all cellular services, including standard voice calls, SMS, MMS, and mobile data. Sensitive and critical functionalities (e.g. wallets, authenticators, NFC, etc.) can be restricted or deactivated once the device is flagged as disabled. Further requirements to protect the data stored on the device are covered later in this document (see section 6.11).

Disabling a device or any associated functions does not imply the override of regulated mandatory services such as emergency call capability or other such functions provided by the device manufacturer. In order to support emergency calls, the device maintains the ability to use GPS and location-based data. This ensures that calls are forwarded to the appropriate local emergency numbers and that emergency responders can identify the device's position.

Req. Number	Requirement
ATH-EME-0010	Disabling a device or any associated functions SHALL NOT override regulated mandatory services such as emergency call capability.

6.2 Location Features

Prior to invoking the device disabling feature the owner or authorised user may seek to locate their device.

Req. Number	Requirement
ATH-LOC-0010	The device locate functions that SHOULD be available to the owner or authorised user are: 1. Emit a loud tone for an extended period to allow the owner or authorised user an opportunity to find the device, assuming it is within earshot.

	2. Display an owner or authorised device user specified message or one chosen from options in the OS on the device lock/home screen. 3. Acquire its location using GPS (or any other location technology if this feature is supported by the device) and transmit this information to the server upon authorised request.
ATH-LOC-0020	The server locate functions that SHOULD be available to the owner or authorised device user are: 1. Signal the device to trigger the emission of a loud tone and confirm that the loud tone is playing. 2. Confirm that the user specified message, or one chosen from options in the OS, on the device lock/home screen has been set. Provide a user interface that allows the owner or authorised device user to retrieve the device's location and display it on a map.

6.3 Out-of-the-box Activation of Key Security Features

When the owner or authorised device user first activates their new mobile device is an opportune time to encourage activation of the anti-theft features, if the owner or authorised device user has not already been automatically opted in. This could be achieved by prompting the new device owner or authorised device user to activate the anti-theft features or by directing the user to additional online or print resources that describe the available features and how they can be activated and used.

Req. Number	Requirement
ATH-ACT-0010	To maximise user protection, anti-theft features (including the device disabling feature) SHOULD be enabled by default, where feasible, with an option to 'opt-out' during the initial device setup process. The owner or authorised device user MUST be clearly informed that these features are active, and MUST be provided with a straightforward option to configure or disable them if they choose.
ATH-ACT-0020	The owner or authorised device user MUST be able to explicitly 'opt-out' of the device disabling feature.
ATH-ACT-0030	During device set-up, and accessible thereafter (e.g., within device settings or help resources), the owner or authorised device user SHOULD be provided with clear, easily understandable information about the supported anti-theft features, how to find them, how they function, how to use them effectively, and any associated privacy implications. All security features SHOULD clearly describe how they relate to one another and the risks that can arise from incorrect configuration. This information SHOULD also highlight which specific anti-theft capabilities are supported by the device model and operating system to aid informed usage.

6.4 Provision of Customer Awareness and Loss/Theft Incident Guidance

Owners and authorised device users need clear and timely guidance in order to use anti-theft features that are easy to use, effective and safe. Information provided only at device set-up may be insufficient in an actual loss/theft scenario, where users may be uncertain which party to contact first, what actions to take, and in what sequence.

Providers of anti-theft features and related support services should therefore ensure that during and after loss/theft incident handling and recovery, owners and authorised device users are given accessible and context-appropriate guidance on available anti-theft capabilities, relevant contact paths, and the recommended sequence of actions.

Customer advice, recommended actions and best practices to protect users against unauthorised device access are described in the 'GSMA Mobile Device Theft - State of Affairs Report' **Error! Reference source not found.**. Furthermore, the requirements described in section 6.18 allow the display of custom messages on a device's locked screen. These messages can be used to facilitate the recovery of a stolen or lost device by enabling the authentication of rightful ownership, and/or by providing return instructions to the finder of the device.

Req. Number	Requirement
ATH-AWR-0010	Owners and authorised device users SHOULD be provided with clear guidance on who to contact in the event of device loss or theft, including, where relevant, the OEM or authorised disablement service, the MNO, law enforcement, and financial or identity-related service providers.
ATH-AWR-0020	Guidance SHOULD explain the recommended sequence of actions following a loss/theft incident, including, where applicable, locate or lock, device disablement, MNO fraud remediation, protection of critical functionalities (e.g. wallets, authenticators, NFC, etc.), service continuity actions, and re-enablement only after legitimate recovery.
ATH-AWR-0030	Customer guidance SHOULD be accessible both at set-up and thereafter during loss/theft incident handling, including through device settings, support resources, or recovery interfaces, and SHOULD be suitable for inexperienced users.
ATH-AWR-0040	Where an MNO is a first point of contact for device theft or loss, the MNO SHOULD provide the owner or authorised device user with a clear and trusted route to the relevant OEM or authorised disablement service, including sufficient information to distinguish the official service from spoofed or fraudulent channels.
ATH-AWR-0050	Providers of anti-theft features and related support services SHOULD provide post-loss/theft incident guidance to the owner or authorised device user on password reset, session revocation, recovery-factor review, and other account hygiene actions following loss, theft, or recovery of a device.
ATH-AWR-0060	Post-loss/theft incident guidance SHOULD also address review of payment, wallet, authenticator, OTP, banking, and identity-related exposure, including when to contact relevant service providers to investigate or mitigate misuse.

6.5 Verify the Authenticity of a Request to Disable Devices

Authenticating the request to disable devices is the first essential step in setting the procedure in motion. A robust mechanism must exist to ensure the identity and authority of the owner or the authorised device user can be established in a manner that is difficult to repudiate. It is recommended that the credentials to be used to invoke the disabling function are distinct from all other accounts.

Req. Number	Requirement
ATH-VER-0010	The owner or authorised device user MUST first be authenticated before proceeding to any next step towards device disablement.

6.5.1 Disabling Feature: Authentication

In the case where the owner or the authorised device user has direct access to disabling features, that access could be authenticated using the most modern industry security standards and would only control the device which is registered to that particular owner or authorised device user.

Req. Number	Requirement
ATH-VER-0020	An owner or authorised device user request to disable a device MUST be authenticated and MUST only control the device which is registered to that owner or the authorised device user.

6.6 Device Can Only be Disabled from an Authorised Server

In a further attempt to prevent device disabling attacks against innocent mobile owners, the triggering of remote disable instructions to target devices must only be permitted from authorised servers, the authenticity of which can be verified.

Req. Number	Requirement
ATH-SER-0010	If a mobile device is disabled remotely, the mechanism to do so MUST only be executed from an authorised server supporting the disable function. In order to fulfil this requirement, the following is needed: • Secure communication between the device and server • Mutual authentication between the device and the server being authorised to perform the function
ATH-SER-0011	In order to detect and react to misuse of the disabling feature, the server SHALL: • Limit the requests to the server to a capped number to prevent misuse • Raise an alarm to highlight the limit has been reached • Send a notification, as appropriate, in the event of suspected misuse of the disabling feature.

6.7 Secure Location and Access to Servers Operating the Disabling Feature

Servers that operate a device disabling feature may be attacked or the staff who have access to information and control mechanisms could be targeted. It is important that these threat vectors are mitigated. Industry experience has shown that a major weakness of the SIM lock feature (which was not designed to be an anti-theft feature), has been the vulnerability of the database servers that store the unlock keys. These servers are targeted for attack and unauthorised access by both internal and external parties who then steal and re-sell the keys for their own benefit. Physical and logical access to the disabling feature servers should be protected from such abuse, in accordance with FS.31 [9] and other industry information security standards such as ISO 27001 [10].

An audit trail must be maintained and available that records ‘disable requests’.

Req. Number	Requirement
ATH-SER-0020	The location, physical and logical access to servers supporting the disabling feature MUST be secure.
ATH-SER-0030	Only authorised personnel SHOULD be allowed to access and invoke the disabling feature.
ATH-SER-0040	The server MUST retain an audit trail of all activities, including all requests received.

6.8 Access to the Disabling Feature

Owners or authorised device users can save time if they can access and invoke a device disabling feature without physical involvement from, or the need for intervention by any other party.

In addition to the owner or authorised device user being able to invoke the disabling of a device if it is misplaced, lost or stolen, a mobile network operator, a distributor or an enterprise could also invoke the disabling of devices lost or stolen from their distribution channel using a similar disabling feature. Further requirements covering re-enablement are covered later in this document (see section 6.9).

Req. Number	Requirement
ATH-DIS-0010	The device owner or authorised device user MUST be able to access and invoke a device disabling feature via the use of self-service capabilities, without needing to involve any other party.
ATH-DIS-0020	The disabling feature SHOULD advise the device owner or authorised device user to contact their MNO if they are concerned that the apps or data on the device or the mobile network service could have been used by someone for fraudulent or malicious purposes e.g. trigger a porting out of their number or initiating an (e)SIM swap, or to make a payment.
ATH-DIS-0030	Once a device owner or authorised device user has successfully disabled their device, the disabling feature SHOULD offer the option to report the device together with the IMEI to the MNO or to law enforcement, banks etc. as being stolen or assumed irretrievably lost.
ATH-DIS-0040	In case the device loss or theft is reported to an MNO by the device owner or authorised device user, the MNO SHOULD advise them to disable their device via the relevant device manufacturer e.g. by providing a link to the device manufacturer’s disabling feature.

6.9 Re-enabling Feature

As temporary loss is far more common than theft, re-enabling device service after a device has been disabled and later recovered is a requirement. This addresses the case where the device is merely temporarily lost.

It is recommended to enforce robust control measures to prevent the accidental re-enablement of disabled devices.

Automatically re-enabling a device exposes it to unnecessary risk. Indefinite disablement ensures that a stolen device is not stored temporarily before being used or resold.

Req. Number	Requirement
ATH-REN-0010	The device MUST have the capability to be re-enabled after it has been disabled.
ATH-REN-0020	The authorised server SHOULD ensure that only the party that invoked the device disabling is allowed to re-enable it.
ATH-REN-0030	The party that invokes the re-enabling of a device MUST authenticate themselves to the authorised server.
ATH-REN-0040	A disabled device MUST remain disabled indefinitely until the device is re-enabled.

6.10 Backup Device Data

The loss of data can have a significant impact on mobile users that fall victim to loss or theft, and backup facilities should be available to allow them to regularly back up their data to secure network servers and to securely retrieve it at a later stage.

Req. Number	Requirement
ATH-BAC-0010	A backup service to a secure network server MAY be offered to the owner or authorised device user. If available, the owner or authorised device user MAY invoke a feature to backup all or selected personal data (i.e., belonging to the owner or authorised device user), residing on the device to a secure network server.

6.11 User Data Protection

In order to protect device data from being accessed by a thief or someone who discovers a lost device there is a need to provide the ability to remotely render the device data inaccessible by wiping it.

Req. Number	Requirement
ATH-WIP-0010	The owner or authorised user MUST have the ability to remotely render all device data inaccessible, such as by wiping.
ATH-WIP-0020	Where remote data wiping is invoked, mechanisms SHOULD be considered to also invalidate or alert relevant services about the potential compromise of OTPs or authenticators that might have been accessible on the device, if technically feasible and supported by service providers.

6.12 Restore and Reload Data and Applications

In the case where a device is disabled and all data and applications are removed, re-enabling the original device will also include reloading and restoring of all data and applications that were backed up and removed from the device as part of the disabling feature.

Req. Number	Requirement
ATH-RES-0010	When restoring functionality to re-enable a device that was previously disabled, the owner's or authorised device user's backed-up data and applications MAY be restored to the device.

6.13 Preservation of Device Stored Data

Device data backed up to the mobile network operator, OEM or 3rd party infrastructure prior to the device being disabled must be stored securely and the confidentiality and integrity of that data guaranteed.

Req. Number	Requirement
ATH-STO-0010	Device data that has been backed-up MUST be stored securely and the confidentiality and integrity of that data MUST be guaranteed.

6.14 Enable Remediation in a Timely Manner

Time is crucial in the case of a lost or stolen device, to protect its data and its unauthorised use. A convenient locking function could be offered for owners or authorised device users to quickly put a device into a locked state, using easy to remember factors such as phone numbers. Further disabling of the device can be carried out with full owner or authorised device user authentication. Once an owner or authorised device user has requested their device to be disabled, they can expect the function to be executed in a reasonable time (i.e. a matter of minutes rather than hours). This is dependent on the device being able to connect to the Internet.

Req. Number	Requirement
ATH-TIM-0010	If an owner or authorised device user has requested their device to be disabled, the disabling feature SHALL start execution once the device is reachable by the server, for example over the Internet.
ATH-TIM-0011	The execution time of the disabling feature SHALL be reasonably short (preferably in the order of seconds).
ATH-TIM-0020	The device MAY be remotely screen-locked by the user, using easily recalled information such as a phone number, and only after easy-to-remember security challenges to guard against potential abuse.
ATH-TIM-0030	MNOs SHOULD advise their customers reporting a device loss or theft to perform remediation actions on their device. The MNO remediation actions applied following the theft report SHOULD be sequenced so as not to unnecessarily prevent the owner or authorised device user from invoking device disablement through the authorised server. This SHOULD be confirmed before any action is performed at the network level that would make the lost or stolen device unreachable on the mobile network e.g. blocking the IMEI, suspending the subscription or applying a bar on data services, unless immediate restriction is required to mitigate active fraud or legal obligation.
ATH-TIM-0040	MNOs SHOULD immediately apply a barring on services that can be abused by an unauthorised third party to impersonate or defraud the victim e.g. messaging and call services.

ATH-TIM-0050	MNOs SHOULD immediately ensure their customer number cannot be (e)SIM swapped or ported out.
ATH-TIM-0060	Where supported by the MNO, the owner or authorised device user reporting theft SHOULD be informed of any available service continuity options for use of a replacement device, and of any conditions necessary to preserve fraud protections and device disablement processes.
ATH-TIM-0070	Where a subscriber's service is moved by the MNO to a replacement device following loss or theft, such reprovisioning SHALL be treated as a high-risk action. Strong authentication, anti-fraud controls, and an audit trail sufficient to support dispute handling and incident review are REQUIRED.

6.15 Ability to Disable a Device When Not Connected to the PLMN

Smartphones have multiple network bearer interfaces (besides mobile, e.g. Wi-Fi, and Bluetooth™) and they can therefore continue to operate without a connection to a mobile network. In fact, most of the functions of a device will remain active. Even voice calls can continue to be made using Over-The-Top services that don't use the mobile network. It is extremely difficult for mobile network operators to reach out and disable a device quickly over the PLMN if the device is exported from its home country and used on a different mobile network. In many cases, especially where a thief wants to continue using a device in the same country, they will immediately remove the mobile network operator's ability to communicate with the device by simply removing the SIM (or eSIM) before continuing to use the device by only using Wi-Fi networks. Therefore, the ability to disable a device that is not connected to a PLMN but is connected to the Internet via another bearer would further deter thieves from targeting mobile devices and will significantly reduce their re-sale value. In addition, devices should support being placed into a disabled state prior to shipment. Refer to section 6.21 for the specific requirements.

Req. Number	Requirement
ATH-CON-0010	Devices SHOULD support receiving a disabling or re-enabling request when they are reachable by the server, for example over the Internet.

6.16 Roamed Devices

A typical scenario is where an owner or authorised device user has travelled outside the home mobile network, for example on a holiday or business trip, and their device is stolen. In this case, the stolen device is registered on a visited mobile network, yet the owner or authorised device user will call their home mobile network operator to report the device stolen. All functions to backup data, disable and restore a device must work for a roamed device. In the case of roaming, the owner or authorised device user may be advised of any additional costs to invoke the function while not on the home mobile network.

Req. Number	Requirement
ATH-ROA-0010	For lost or stolen devices registered on a visited mobile network (roaming), all functions for backing-up data, disabling the device and restoring the device MUST still function successfully.
ATH-ROA-0020	For lost or stolen devices registered on a visited mobile network (roaming), the device owner or authorised device user may be advised

	by the disabling function of any additional costs when attempting to invoke functions to back-up data, disable the device or to restore the device.

6.17 Prevention of Unauthorised Device Re-initialisation

Attempts by criminals to get access to disabled devices will continue and likely increase. To the extent that it is technologically feasible, a disabled device needs to be hardened against physical tampering aimed at bypassing on-device security and have software and hardware security mechanisms that are sufficiently robust to resist and deter attempts to break into the data or re-enable the device. Basic logical engineering measures such as not allowing the use of “factory reset” functions to be used on disabled devices are part of an overall important package of measures designed to prevent the re-enablement of stolen devices.

Device manufacturers need to continue to implement and constantly evolve measures to deter and prevent the unauthorised re-initialisation of a lost or stolen device to a state where it can be used by someone other than the owner or authorised device user. This includes measures to resist and effectively prevent the exploitation or bypass of anti-theft features. State of the art solutions from component providers should be used to achieve this critical goal.

Note: Re-initialisation includes using factory reset, operating system re-install, and re-flash of the device boot loader to bypass the owner or authorised device user credentials. Included in this is the need to prevent tampering with the device firmware (boot-ROM) or other data, such as the IMEI, that would be necessary to legitimise the operation of a device. This element is further described in section 6.19. Device re-initialisation for legitimate purposes e.g., re-sale, needs to be available to the owner. For Mobile Device Management (MDM) administered, pool or supervised Corporate-Owned, Personally-Enabled (COPE) devices, this needs to be local to corporate or company policy and, as such, is out-of-scope of this recommendation document.

Req. Number	Requirement
ATH-UNA-0010	It SHALL NOT be possible to bypass active anti-theft measures, including by means of factory reset, bootloader unlocking, OS re-flashing, device firmware modification, or similar re-initialisation procedures.
ATH-UNA-0011	ATH-UNA-0010 SHOULD be supported by a hardware-backed Trusted Execution Environment (TEE) to prevent tampering and unauthorised reset, hindering stolen device resale and reuse.
ATH-UNA-0012	Device re-initialisation for legitimate purposes e.g., re-sale, SHOULD be available to the owner. Legitimate re-initialisation procedures MUST be securely authenticated and auditable.

6.18 Home/Lock Screen Display Message

The display of messages, highlighting the fact that a device has been lost or stolen to third parties that later seek to use the device, may be useful as a deterrent.

Req. Number	Requirement
ATH-HOM-0010	A function to display a custom message on the home/lock screen of the device when the device is not in the owner's or authorised device user's possession SHOULD be made available.
ATH-HOM-0020	If set by the owner of a device or the authorised device user, a custom message SHOULD be displayed to third parties, that later seek to use the device when it is not in the possession of the owner or authorised device user.

6.19 Securing IMEI

The integrity of the IMEI is fundamental to many network-based and device-based anti-theft measures. Device manufacturers need to implement robust hardening mechanisms to ensure the IMEI programmed into the device is immutable and cannot be altered through software or physical electrical and software tampering methods. When the IMEI is transmitted to the network or displayed, it needs to originate from a secure, non-modifiable hardware component or protected storage as required by 3GPP TS 22.016 [12] and GSMA TS.06 [8]. As mentioned in section 6.17, device manufacturers need to continually evolve and maintain security measures in devices to help deter theft. Further material on hardware and software security device security measures can be found in GSMA's IMEI Security Technical Design Principles [13] and OMTP TR1 [11].

Note: It needs to be considered that counterfeit or so-called 'Shanzhai' devices might contain invalid and duplicate IMEIs (stolen from existing TAC ranges, which are public information). These invalid IMEIs might therefore also match genuine, authentic devices on a mobile network. Solutions involving IMEI numbers need to consider how to investigate and handle scenarios where a duplicate is discovered, and how best to identify authentic devices.

Req. Number	Requirement
ATH-IMEI-0010	Device manufacturers SHALL ensure that the IMEI (or IMEIs, in the case of multi-SIM devices) programmed into a device at the point of manufacture is unique as per 3GPP TS 22.016 [12] and GSMA TS.06 [8], and is also cryptographically and physically protected against unauthorised modification.
ATH-IMEI-0020	The mechanism storing the device IMEI(s) SHALL resist tampering, i.e. manipulation and change, by any means (e.g. physical, electrical and software) aimed at altering or erasing the IMEI as per 3GPP TS 22.016 [12] and GSMA TS.06 [8].
ATH-IMEI-0030	When the device transmits its IMEI(s) to a PLMN over the air interface, the IMEI(s) SHALL originate from the secure, non-modifiable hardware component or protected storage referenced in ATH-IMEI-0010 and ATH-IMEI-0020.
ATH-IMEI-0040	When the device software displays the IMEIs (e.g., in settings, on a lock screen, or when disabled), the displayed IMEI(s) SHALL be read directly from the same secure, non-modifiable source from which it is transmitted to the network.
ATH-IMEI-0050	If the device supports other persistent hard-bound identifiers (e.g., EID for eSIMs) relevant to anti-theft and network identification, similar

	integrity protection mechanisms as above SHALL be applied to those identifiers.

6.19.1 Identifying IMEIs of Disabled Devices

There are a number of scenarios where the IMEI can be useful in identifying if the device has been stolen or barred from service. This is especially useful for third parties when a device is recovered and returned to a police station or at device recycling centres, lost property offices or if the device is sold at a second-hand shop or online auction / re-sale site, etc. It is not desirable for devices to be irrecoverable or non-returnable to their legitimate owner or authorised device user. Phones are the centre of everyone's lives and the loss of access to services such as email or banking is a big problem. The data on phones is highly personal; the loss of photos, videos and other data can be extremely distressing for users. It is therefore in everyone's interests that as many devices that can be, are returned to users, and as soon as possible.

Devices need to display the IMEI on the display screen once the device has been disabled. Maintaining access to the IMEI of a disabled device is essential for reconnecting it to the rightful owner as its knowledge facilitates investigations into thefts and enables real-time verification of whether the device has been reported as lost or stolen **Error! Reference source not found.**. In addition, an option to include the visual display of a Code 128 barcode representation of the IMEI number on the device display would allow for the automatic reading of the number, thus avoiding mistakes caused by human error. Note that 3GPP TS 22.030 also defines the procedure for the presentation of the IMEI and e-marking on devices [14].

A trend towards the removal of the physical printed IMEI number and accompanying Code 128 barcode on devices by manufacturers also impedes recovery of both lost and stolen devices, especially in the likely scenarios where the device is out of battery or the screen of the device is damaged. This provides a negative user experience and contributes to unnecessary e-waste. Manufacturers need to re-consider such decisions in light of the critical impact that lost and stolen devices have on users.

In addition to displaying the IMEI, a disabled device may support a recovery service operated by the authorised disablement server. Such a service can assist legitimate third parties, for example law enforcement, lost-property offices, recyclers, retailers, repairers, or other authorised handlers, in identifying that a device is in a disabled, lost or stolen state and in routing that device into an official recovery process.

The recovery service may use the IMEI or a privacy-preserving machine-readable recovery reference, such as a QR code or NFC token, to provide a trusted path for status verification, notification of the owner or authorised device user, and verification of entitlement before return or re-enablement. Implementations should minimise unnecessary disclosure of personal data and reduce risks associated with spoofing, phishing, or other misuse.

If displaying a QR code, appropriate measures should be taken to avoid this becoming a vector for user exploitation (e.g., by malware or spyware, a technique sometimes known as 'Quishing' or QR Phishing). Ensuring that the user is fully aware of the destination URL and accompanying information about its purpose will help to alleviate user concerns about scanning a QR code.

Req. Number	Requirement
ATH-DIS-0050	The device IMEI (and other relevant persistent device identifiers like EID if applicable) SHALL be accessible or displayable when the device is disabled. The implementation details are left to the OEMs. NOTE: Clear instructions for an inexperienced user on how to obtain the IMEI of a disabled device SHOULD be readily available (e.g., via manufacturer support websites.
ATH-DIS-0051	To complement the display of the IMEI, devices in a lost or disabled state MAY provide a privacy-preserving recovery reference, such as a QR code or NFC token, linking to a recovery service operated by the authorised disablement server.
ATH-DIS-0052	Recovery services based on recovery references SHALL provide a mechanism for legitimate third parties to use the recovery reference to verify that the device is in a disabled, lost, or stolen state.
ATH-DIS-0053	A recovery service SHALL minimise unnecessary disclosure of personal data and SHALL include measures to reduce risks of spoofing, phishing, misuse of recovery references, and unauthorised check of device status.
ATH-DIS-0054	Where a recovery event is registered, the service SHOULD notify the owner or authorised device user through established account channels, without unnecessarily disclosing personal data to the originator of the recovery event.

6.19.2 IMEI Display on Screen-locked Devices

For screen-locked devices, display of the device IMEI might not require specific knowledge of the device user interface.

- When a device is screen-locked, IMEI display is easy to accomplish through a few user actions (e.g., clicks/button presses, swipes, etc.) without the user being authenticated to the device.
- Clear instructions for an inexperienced user on how to obtain the IMEI are shown.

Examples of obtaining IMEI display from a screen-locked device may include:

- The IMEI can be displayed as part of the mobile device locked screen.
- There can be a “request IMEI” option on the mobile device locked or mobile device disabled screen.
- Looking at the printed IMEI number on the device itself.
- When an emergency call is initiated from a device locked screen, a pre-call window (emergency dialogue box) appears asking the user if they really want to make an emergency call. In that dialogue box the IMEI can be displayed.

A recovery service operated by the authorised disablement server may also provide a privacy-preserving communication channel between the finder of a locked device and the owner or authorised device user. For example, where a finder uses the IMEI or a privacy-preserving recovery reference such as a QR code or NFC token to access the official recovery service, the service may enable messages to be relayed between the parties to arrange recovery without unnecessarily disclosing personal identifiable information of either

party. Such a mechanism can help support safe return of the device while reducing risks of spoofing, phishing, harassment, or other misuse.

Note: If displaying a QR code, appropriate measures should be taken to avoid this becoming a vector for user exploitation (e.g., by malware or spyware, a technique sometimes known as 'Quishing' or QR Phishing). Ensuring that the user is fully aware of the destination URL and accompanying information about its purpose will help to alleviate user concerns about scanning a QR code.

Req. Number	Requirement
ATH-DIS-0060	The device MUST provide functionality to display the IMEI(s) on its screen as a numeric string and a Code 128 barcode, where supported by the device form factor, even in screen-locked mode and without user authentication. The IMEI MUST be retrieved from the device's hardware as outlined in ATH-IMEI-0040. This functionality SHOULD be enabled by default. An option to disable this functionality MAY be provided to the user.
ATH-DIS-0070	To complement the display of the IMEI(s) on a locked device with device disablement capability, devices MAY provide a privacy-preserving recovery reference, such as a QR code or NFC token, linking to a recovery service operated by the authorised disablement server. Where such a reference is provided, the linked service SHOULD support trusted status verification and routing into an official recovery process, while minimising unnecessary disclosure of personal data and reducing risks of spoofing, phishing or misuse.

6.20 Advanced Device Protection and Disablement Requirements

Building upon the general disabling features, advanced device protection mechanisms need to be designed and in place to be resilient against attacks.

Proactive protection mechanisms need to be considered, such as detection of suspicious reset attempts or unusual location changes post-disabling request.

Req. Number	Requirement
ATH-KSW-0010	A device SHOULD detect when it is separated from its authorised user and lock its screen(s) to protect the data.
ATH-KSW-0020	Remotely disabling or re-enabling the device relies on network connectivity. Attackers commonly disconnect stolen devices to avoid owner or authorised device user actions. A device SHOULD implement protection to detect when it is taken offline for a prolonged period and proactively lock its screen to protect its data. Privacy aspects such as exposing the device online/offline status SHOULD be considered when implementing this functionality.

6.21 Supply Chain Protection

Some thefts within the supply chain can take time to be discovered and reported. The device could be disabled when in storage or during transport:

1. To prevent stolen devices from being resold before they can be disabled and
2. To protect stolen device components from being repurposed in other devices, see section 7.2.

A similar approach can also be adopted to protect a used device during its transport, for example to send it for servicing or to a new owner.

Supply chain scenarios include the pre-disabling of devices on a per IMEI basis before they leave the factory or an upstream distribution hub. The IMEI is most commonly used as an identifier but other device identifiers can also be used. For example, an MNO, enterprise or reseller may place a purchase order for a batch of devices and, as part of the fulfilment process, receive from the OEM a digital record of the IMEIs associated with that order. These IMEIs can then be imported into, or registered with, the OEM disablement portal so that each device is placed into a disabled state prior to shipment. Once the batch has been safely received into a secure location such as a warehouse, retail outlet, corporate staging facility, or once an individual device has been delivered to the intended end customer, the party who performed the order (MNO, enterprise, reseller) can use the same interface to re-enable the corresponding devices.

This model has the potential to reduce the motivation for supply chain theft and reduces the resale value of intercepted devices, as any device removed from the legitimate distribution path remains disabled until re-enabled by the authorised party. The same approach can be applied to second-hand and refurbished devices moving between repair centres, grading facilities, resellers and end customers, ensuring that devices remain disabled while in storage or transit and are only re-enabled when under the control of the intended recipient.

Req. Number	Requirement
ATH-SUP-0010	Supply chain actors authorised to act on devices or batches prior to end-user receipt, or during authorised servicing, refurbishment, or resale preparation, SHOULD be authenticated as part of the onboarding process that defines their roles, permissions, and scope of authority.
ATH-SUP-0020	Where supply chain protection is supported, the authorised server SHALL support the association of devices, identified for example by IMEI and, where relevant, EID, with an authorised supply-chain actor, recipient, batch, order, or other legitimate supply chain reference sufficient to support authorised disablement and re-enablement decisions.
ATH-SUP-0030	Devices SHOULD support being placed into a disabled state prior to being shipped, including when the device has no internet connectivity.
ATH-SUP-0040	Where a device has been placed into a supply chain disabled state, that disabled state SHOULD be maintained throughout custody transfer until re-enabled by an authorised server.
ATH-SUP-0050	An authorised supply-chain actor reporting supply chain theft, loss, diversion, tampering, or other exception affecting protected devices SHALL be authenticated before the authorised server accepts a request to apply, maintain, or update the disabled state of the affected device(s).
ATH-SUP-0060	Where supply chain protection is supported, the authorised server SHALL retain an audit trail of supply chain state changes and related

	requests, including sufficient information to support incident review, and dispute handling.
ATH-SUP-0070	The authorised supply-chain actor SHALL re-enable the device only after confirmation that it has been received into the custody of the legitimate recipient or other authorised service party.

6.22 Universal Access

Device disabling features should be rolled out in all markets to avoid creating geographical regions where criminals are more incentivised and motivated to steal devices to export them globally. Device disabling features should be available to as many mobile users and MNOs as possible.

Req. Number	Requirement
ATH-UNI-0010	Device disabling features SHOULD be implemented globally in all markets and provided to all mobile users and MNOs.

6.23 Provision of Supply Chain Actor Awareness

Supply chain anti-theft measures involve multiple operational actors and hand-off points. Effective supply chain protection therefore depends not only on device disablement and identifier integrity, but also on clear awareness of roles, reporting routes, escalation paths, verification procedures, and re-enablement conditions.

Providers and participants in supply chain anti-theft processes should ensure that authorised supply chain actors are onboarded appropriately and provided with clear operational guidance for theft reporting, custody handling, legitimacy verification, and recovery or re-enablement processes.

Req. Number	Requirement
ATH-SAW-0010	Authorised supply chain actors SHOULD be provided with clear guidance on their roles, permissions, and escalation paths for supply chain theft scenarios, including theft in transit and theft in storage.
ATH-SAW-0020	Supply chain guidance SHOULD identify which parties are authorised to report theft, maintain or request device disablement, verify recovered devices, and request re-enablement, and under what authenticated conditions those actions are taken.
ATH-SAW-0030	Where IMEI, EID, or machine-readable recovery or custody references are used in supply chain scenarios, guidance SHOULD explain their intended use, how legitimacy is to be checked, and how affected devices are to be routed into the correct authorised process.

7 Further Study

The topic of device theft is ever evolving. As security measures are deployed, criminals develop new techniques and different business models in order to steal devices or to be able to extract value from the stolen items. This section looks at areas for future study by industry.

7.1 Tackling Unauthorised Device Dismantling and Reassembly

Devices are often stolen, fenced and subsequently dismantled for parts, which results in situations where components from other devices are re-used to create so-called 'frankenphones'. The information on what physical components make up the original device is often not available or not in a common, standardised format. A Hardware Bill of Materials (HBOM) is a tool to address the unauthorised device dismantling and reassembly. This topic is beyond the scope of these device anti-theft requirements but is a related subject and further exploration by GSMA members is encouraged.

7.2 Component Reuse Protection

Thieves often disassemble stolen or disabled devices to resell working parts (e.g., screens, batteries, motherboards). To reduce the residual value of stolen devices and their components, devices can implement parts binding checks so that critical components removed from a disabled device cannot be used in another device without authorised reprovisioning. These mechanisms can leverage hardware identities and OEM attestation. They can be designed to preserve emergency service access and support legitimate repairs and sustainability goals.

When a device is placed into a disabled state, it may be able to mark its paired critical components as quarantined or disabled so they cannot be repurposed in other devices. Note that this requirement and other hardening methods existed as security requirements in the mobile industry's work to fight handset theft in OMTP TR1 in 2009 [11].

7.3 Device Identifier in Recovery Process for Lost/Stolen Devices

This specification uses the IMEI as a means to identify the rightful owner of lost or stolen devices, primarily due to its standardisation as the unique identifier of Mobile Equipment in ETSI/3GPP and its compatibility with existing databases and services that rely on the IMEI (e.g., GSMA Device Registry, MNO subscriber database, etc.). However, as a static and immutable identifier, exposing the IMEI to unauthorised device holders may lead to risks such as IMEI harvesting, unnecessary data disclosure, or device/user tracking.

To address these concerns, the mobile industry could develop an integrity-protected, privacy-preserving, time-varying yet unique device identifier dedicated to the recovery process for lost or stolen devices. Developing such an identifier is left for further study, as it falls outside the scope of this specification and requires collaboration among a much broader set of interested parties beyond GSMA.

7.4 Device Service Repair

The device servicing and repair supply chain may become a source of weakness where stolen devices are concerned. The mobile industry could consider measures to ensure that where devices are transferred to an authorised repair centre, refurbishment facility, or similar authorised service party, re-enablement or controlled servicing access should only be available within the scope of that actor's authorised role and would not weaken the requirement that the device remains protected against unauthorised reuse, diversion, or release.

Annex A Matrix Mapping Requirements to Actors

This table provides an easy look-up guide for readers who wish to understand the roles by different actors involved where they are required to interact or take action.

NOTE: Manufacturer also includes the Operating System and other components of the device, which may be provided by other suppliers.

Requirement(s)	Owner / Authorised Device User	Manufacturer	Operator	3rd Party	Notes
6.1 Disabled Device Functionalities: **ATH-EME-0010**		X	X		
6.2 Location Features: **ATH-LOC-0010 -> 0020**	X	X	X	X	Implementation dependent
6.3 Out-of-the-box activation of key security features: **ATH-ACT-0010 -> 0030**	X	X			
6.4 Provision of customer awareness and loss/theft incident guidance: **ATH-AWR-0010 -> 0060**		X	X	X	
6.5 Verify the authenticity of a request to disable devices **ATH-VER-0010 -> 0020**	X	X	X	X	Implementation dependent
6.6 Device can only be disabled from an authorised server: **ATH-SER-0010 -> 0011**		X	X	X	Implementation dependent
6.7 Secure location and access to servers operating the disabling feature: **ATH-SER-0020 -> 0040**		X	X	X	Implementation dependent
6.8 Access to the disabling feature:	X	X	X	X	Implementation Dependent

Requirement(s)	Owner / Authorised Device User	Manufacturer	Operator	3rd Party	Notes
ATH-DIS-0010 -> 0040					
6.9 Re-enabling feature: **ATH-REN-0010 -> 0040**	X	X	X	X	Implementation dependent
6.10 Backup device data: **ATH-BAC-0010**	X	X	X	X	Depends on where and how data is stored
6.11 User data protection: **ATH-WIP-0010 -> 0020**	X	X	X	X	Implementation dependent
6.12 Restore and reload data and applications: **ATH-RES-0010**	X	X	X	X	Implementation dependent
6.13 Preservation of device stored data: **ATH-STO-0010**		X	X	X	Implementation dependent
6.14 Enable remediation in a timely manner: **ATH-TIM-0010 -> 0070**	X	X	X	X	Implementation dependent
6.15 Ability to disable a device when not connected to the PLMN: **ATH-CON-0010**		X			Implementation dependent
6.16 Roamed devices: **ATH-ROA-0010 -> 0020**	X		X		
6.17 Prevention of unauthorised device re-initialisation **ATH-UNA-0010 -> 0012**		X			
6.18 Home/lock screen display message **ATH-HOM-0010 -> 0020**	X	X	X		Implementation dependent

Requirement(s)	Owner / Authorised Device User	Manufacturer	Operator	3rd Party	Notes
6.19 Securing IMEI **ATH-IMEI-0010 -> 0050**		X			Implementation dependent
6.19.1 Identifying IMEIs of disabled devices **ATH-DIS-0050 -> 0054**		X			Implementation dependent
6.19.2 IMEI display on screen-locked devices **ATH-DIS-0060 -> 0070**		X			Implementation dependent
6.20 Advanced device protection and disablement requirements: **ATH-KWS-0010 -> 0020**		X			
6.21 Supply chain protection: **ATH-SUP-0010 -> 0070**	X	X	X	X	
6.22 Universal access: **ATH-UNI-0010**		X	X	X	
6.23 Provision of supply chain actor awareness: **ATH-SAW-0010 -> 0030**	X	X	X	X	

Annex B Mobile Device Anti-Theft Legislation

Proposed legislation has emerged from a variety of sources and at a variety of levels, e.g., state and federal in the USA, that seeks to mandate the provision of capabilities on mobile devices for the specific purpose of theft prevention. Legislation has been enacted in the US states of California, Connecticut and Minnesota and although the nature of what is being called for has varied significantly in some of the detail, and the potential for conflicting requirements exists, the various legislative proposals have some general common technical requirements. The California legislation includes the following additional aspects:

- Legislation only applies to smartphones
- Render the essential features of the device inoperable / inaccessible to mobile networks
- Prevent reactivation of the device unless by the owner or owner's designee
- Disabling must be reversible by the owner
- Withstand hard reset
- All smartphones manufactured after a specified date must include this feature

Annex C Document Management

C.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	22/05/14	New PRD SG.24	PSMC	David Rogers, Copper Horse
2.0	18/05/15	Revised version taking into account feedback provided by Apple, Blackberry, Huawei, Microsoft, Qualcomm and Samsung. An additional requirement was added to ensure the IMEI can be displayed on locked/killed devices.	FASG	Nicholas Alfano, Blackberry
3.0	17/05/16	Revised version taking into account feedback from DSG members.	FASG	James Moran, GSMA
4.0	17/07/26	Revised version includes latest anti-theft features developments, supply chain security requirements, provision of customer awareness and incident guidance, and provision of supply chain actor awareness.	ISAG	James Moran, GSMA

C.2 Other Information

Type	Description
Document Owner	Fraud and Security Group
Editor / Company	Nataliya Stanetsky, Google

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.