

Anti-Theft Device Feature Requirements
Version 1.1
16 December 2014

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2014 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction 3
2 Definitions, Abbreviations and Requirements Format 3
2.1 Definitions 3
2.2 Abbreviations 4
2.3 Requirements Format 4
3 Scope 5
4 Network Based Anti-Theft Mechanisms 6
4.1 Network Based Anti-Theft Solutions 6
5 Proposed Legislation for Mobile Device Anti-Theft Features (Kill Switch) 7
5.1 Kill Switch Background and Concerns 7
5.2 Device Anti-Theft Features and IMEI Blocking 7
5.3 Mobile Device Anti-theft Legislation 8
6 Requirements for a Mobile Device Disablement and Restore Feature 9
6.1 Emergency Calling Provision 9
6.2 Location Features 9
6.3 Out-of-the-box Activation of Key Security Features 10
6.4 Verify the Authenticity of a Disablement Request 10
6.4.1 Authentication by Network Operator 10
6.4.2 Authentication by Owner 10
6.5 Device can only be Disabled from an Authorized Server 11
6.6 Secure Location and Access to Servers Operating the Disabling Feature 11
6.7 Owner Access to the Disabling Function 11
6.8 Restore Service Function 12
6.9 Backup Device Data 12
6.10 Device Data Protection (Device Wipe) 12
6.11 Restore and Reload Data and Applications 12
6.12 Preservation of Owner Stored Data 13
6.13 Execute the Disable Function in a Timely Manner 13
6.14 Ability to Disable a Device when not Connected to the PLMN 13
6.15 Roamed Devices 14
6.16 Prevention of Unauthorized Device Re-initialization 14
6.17 Home/Lock Screen Display Message 14
Annex A Matrix Mapping Requirements to Actors 16
Annex B Document Management 18
B.1 Document History 18
B.2 Other Information 18

1 Introduction

To date there have been various efforts and a variety of approaches taken to address the issue of mobile phone theft. Some include technical capabilities and processes implemented by network operators to control device access to their networks via IMEI validation using Equipment Identity Registers (EIRs) and the sharing of blacklisted IMEIs by connecting EIRs to GSMA's IMEI Database. These solutions are outlined in Section 4: Network Based Anti-Theft Mechanisms and they have been in place for many years. They continue to be improved and extended.

Recently, the increase in 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 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 discussed and summarized in Section 7: Proposed Legislation for Mobile Device Anti-Theft Features (Kill Switch).

Mindful of the fact that a range of stakeholders, including users have a role to play to combat handset theft, Section 9: Service, describes mechanisms to assist handset owners to combat and protect themselves from theft. These mechanisms include the ability to disable service to a mobile device and restoring the device to an operational state if the device is returned to its rightful owner. In addition, various anti-theft features that are currently offered by handset manufacturers, a list of third party tools that can be used to locate lost devices and other resources consumers can use to safeguard their devices and data from theft are located on the GSMA's website at: http://www.gsma.com/technicalprojects/fraud-security/security-advice-for-mobile-phone-users/mobile-phone-theft

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
Device Hardware	The physical components that together make a functioning mobile device including screen, keys, printed circuit board, chips, SIM card, removable storage, etc.
Device Software	All software programs on the device and SIM card, including applications, operating system, boot loader, boot-ROM, and firmware.
Owner	The authorized owner and user of the device. Typically this would be the same individual who purchased the device, but there are many variations on this and the purchaser may be a spouse, parent or employer where the device is given to a partner, child or employee. During the device out-of-the-box activation process (including if the device is legitimately factory reset), the owner will need to enter information that is unique to themselves and identifies them as the authorized owner and user of the device. Normally, a username and password would be part of this activation.

	Throughout this document the owner will also imply the legitimate user of the device with the assumption there is only one owner, although there may be variations.
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 network, by means of using a network of another operator.

2.2 Abbreviations

Abbreviation	Definition
3G	A third generation mobile network (for example UMTS)
3GPP	3rd Generation Partnership Project: www.3gpp.org
CEIR	Central Equipment Identity Register (the former name of the IMEIDB)
EIR	Equipment Identity Register
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GSMA	The GSM Association – www.gsma.com
IMEI	International Mobile Equipment Identity
IMEIDB	The GSMA IMEI Database (formerly called the CEIR)
ISP	Internet Service Provider
MSISDN	Mobile Station International Subscriber Directory Number (a telephone number)
OS	Operating System
PLMN	Public Land Mobile Network
ROM	Read Only Memory
SEIR	Shared Equipment Identity Register – sometimes a subset of the data on the IMEIDB within a group of 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 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 phone industry towards a mechanism that would allow the remote disabling of service to a mobile device requires a structured approach and assessment of the problem. Ad hoc solutions proposed in government legislation, or defined by individual manufacturers or operators will inevitably create an inconsistent service experience for users worldwide and will allow theft to continue largely unabated as criminals will be able to exploit weaknesses in these efforts. The GSMA, as it represents over 1,000 network operator and supplier companies in more than 220 countries, can address the fragmentation challenge by defining a feature, by achieving consensus of its membership, that could lead to a consistent implementation of a worldwide solution that is widely supported by operators and device manufacturers. To achieve this objective the optimal approach is to set requirements, define an architecture, and finally define protocols and procedures to implement.

This document defines a set of requirements which can be used by mobile device manufacturers, network operators, and third party service providers, to offer a set of features to device owners to assist in locating lost/stolen handsets and to protect the data within the handset. 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 vendors may choose to embed these features in the operating system. The implementation of these features may also require support from network operator infrastructure or other third party or manufacturer provided servers that are accessible to device owners 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, but at the same time leave the handset manufacturers, 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 all handsets offer similar and consistent anti-theft features.

The scope of work in this document is focussed on securing the legitimate owner’s device and data using software features available on the device and/or within the network. It is not in the scope of this document to address situations when the device hardware or IMEI integrity is compromised through tampering, disassembly/re-assembly, etc. A requirement at the end of this document does, however require the continued attention to and evolution of such measures within the context of an ever-shifting threat landscape.

The effectiveness and efficiency of all anti-theft features are directly linked to and 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 on the capacity of the device manufacturers, and their suppliers, to deliver strong and robust platforms.

Further details on the mobile industry's previous work in this area can be found in the following documents:

- OMTP Advanced Trusted Environment: OMTP TR1
- OMTP Security Threats on Embedded Consumer Devices
- OMTP Trusted Environment: OMTP TR0
- Security Principles Related to Handset Theft (better known as 'the 9 principles')
- IMEI Security Weakness Reporting and Correction Process

4 Network Based Anti-Theft Mechanisms

Network based approaches to anti-theft are briefly outlined in this section. The network operator's primary tool used to prevent the connection and use of stolen or counterfeited devices is the Equipment Identity Register (EIR), which contains a domestic blacklist and the sharing and consolidation of blacklists from multiple operators from various jurisdictions via the GSMA's IMEI Database. These capabilities are used to block devices from receiving service based on the IMEI transmitted by the device to the 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 network is allowed or blocked based on validating 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 network to another by sharing their individual blacklists. This has been accomplished in many countries via a shared EIR (SEIR). Connection to the GSMA IMEI Database and use of its data in individual operator EIRs is an important and valuable resource to block stolen devices from accessing domestic and overseas networks so as to reduce the cross-border trafficking of stolen devices. Operators can export their stolen lists to contribute to the content of the GSMA IMEIDB and thereby facilitate the widest possible 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 Proposed Legislation for Mobile Device Anti-Theft Features (Kill Switch)

5.1 Kill Switch Background and Concerns

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 phone theft. While a clear definition of what constitutes a “Kill Switch” was never put forward and therefore remains unclear, it implies some mechanism to remotely disable or “kill” a mobile phone once it has been stolen or otherwise no longer in the possession of the rightful owner. In the absence of a definition from the media and politicians, GSMA put forward the following definition:

A 'Kill Switch' is a way to disable all functions of a mobile phone or device. It is essentially a function within the mobile equipment, so that if a message of some format (such as a special SMS) is sent to it, then the mobile will cease to operate, and cannot be reactivated or reused.

A centralised mechanism built into the GSM/3G 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 cyber security risk to the mobile industry and users. As such, the GSMA Security Group has advised against the development of this capability due to the significant denial of service attack vector that would emerge.

As an alternative, the GSMA Device Security Steering Group developed this document as a guide to device manufacturers, network operators and governments on how a consistent set of features can be invoked by a device owner to track, disable, and re-enable their device if it is misplaced, lost or stolen. These features are invoked by the authorized owner of the device and can only be applied to the handset registered to the owner. The implementation of these capabilities and tools will be done by device manufacturers (and other industry service providers) and while the features will be similar across mobile devices, the implementation can, and is likely to, be different for each device vendor. This de-centralization of the disabling function down to the user level will make it difficult for any unauthorized 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 their products, but providing similar features across all manufacturers to assist the owners in retrieving their devices and/or safeguarding the device data is the ultimate objective of the recommendations and requirements described in this document.

It should be noted, that the CTIA in the USA developed the “Smartphone Anti-Theft Voluntary Commitment”, which was released on the 15th of April 2014. This document is aligned to all of those commitments and does not have any conflicting requirements.

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. Network operators will continue to use the EIR and IMEI Database to block network service to blacklisted IMEIs. Blocking an IMEI only stops the device from obtaining wide-area cellular service in the region in which it is invoked.

Smartphones can continue to operate over Wi-Fi in a “data only” mode and thus would continue to be usable and have value as stolen items. Similarly, devices are free to connect to mobile app stores and servers to perform software upgrades and access the latest applications etc, thereby preserving the functionality and value of stolen devices. Additionally, IMEI blocking does not preserve or protect the owner’s data on the device. The features outlined in this document will complement the IMEI blocking service and give owners additional tools to protect their data on the device and to retrieve the device in a way that IMEI blocking cannot.

5.3 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. 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 common technical requirements and these are as follows:

- Render the device inoperable / inaccessible to mobile networks
- Prevent reactivation of the device unless by the rightful owner
- Must wipe all user data
- Wiping and disabling must be reversible by the rightful owner
- Withstand hard reset
- All devices sold and/or manufactured after a specified date must include this feature

In addition one piece of draft legislation also proposed a requirement to “*disable the device, even if it is turned off with SIM / storage card removed”*. While it is not clear what the legislators have in mind for this requirement, it would be technically difficult to invoke any action on the device if the device had no connectivity to any network, whether that be the wide-area cellular network or connectivity to the Internet via Wi-Fi or a cabled connection. With no connectivity available to the device the only option for disabling it would be at the network level by using the features discussed in Section 4.

In the following section, requirements for a theft prevention feature are provided and all the above common technical requirements are addressed. Further study is needed on the ability to address the challenges identified in relation to disabling a device that is powered off and has no connectivity to a PLMN.

6 Requirements for a Mobile Device Disablement and Restore Feature

The basic model behind these requirements envisages the involvement of the owner and the network operator as the two actors involved in the execution of the disablement feature that renders all functions on a device useless and unusable, other than emergency service access as defined in section 6.1.

The first working scenario is where the owner, having become aware their handset is missing (be it stolen or misplaced), decides to contact their service provider to request that the device be disabled.

The second scenario is where the owner has direct access to a disabling tool via a web site interface or application available on their home computer or alternate mobile device.

6.1 Emergency Calling Provision

Disabling of service to a device does not imply the override of regulated mandatory services such as emergency call capability or other such functions provided by the device manufacturer or OS provider.

Req. Number	Requirement
ATH-EME-0010	Disabling of service to a device shall not override regulated mandatory services such as emergency call capability and if supported, emergency numbers programmed by the owner (such as “phone home”).

6.2 Location Features

Prior to invoking the device disabling feature the owner should make all attempts to locate their device. Frequently, a device is not lost but merely misplaced. Therefore, prior to disabling the device the owner should attempt to locate it.

Req. Number	Requirement
ATH-LOC-0010	Three locate functions that should be available to the owner are: 1. Signal the device to emit a loud tone for an extended period (30 seconds to 3 minutes) to allow the owner an opportunity to find the device, assuming it is within earshot. 2. Display a message on the device lock/home screen asking for return of the device. 3. Find the location of the device using GPS (or any other location technology if this feature is supported by the device) and show the location on a map. If these features do not find the device or confirm the device has been irretrievably lost or stolen (e.g. GPS coordinates show the device in a location unknown by the owner), then the procedure to disable service can be invoked by the owner.

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

Given that when the owner first activates their new mobile device is the point in time when they fully engage in learning how to operate it, this would be an opportune time to educate the user on anti-theft features and behaviours. One possible approach would be to make it mandatory for the new device owner to step through a short tutorial on anti-theft features and general safe behaviour when using and storing the new device. Completion of the tutorial could be mandated as being necessary before service activation.

Req. Number	Requirement
ATH-ACT-0010	The device, on initial start-up and setup must explicitly guide the owner through the setup of anti-theft features and any other relevant security features such as device access control mechanisms.
ATH-ACT-0020	The owner must be able to explicitly 'opt-out' of the device disabling feature but must, as a default, be 'opted-in'.
ATH-ACT-0030	On initial start-up and set-up, a short tutorial should be shown to the owner to educate on general safe behaviour when using and storing the new device. Completion of the tutorial should be made necessary before service activation.

6.4 Verify the Authenticity of a Disablement Request

Authenticating the request to disable a device is the first essential step in setting the procedure in motion. A robust mechanism must exist to ensure the identity and authority of the rightful owner can be established in a manner that cannot be repudiated.

Req. Number	Requirement
ATH-VER-0010	The request to disable a device must be verified as authentic before proceeding to any next step towards device disablement.

6.4.1 Authentication by Network Operator

A request from a device owner to a network operator to disable a device must be authenticated, otherwise it would be possible for any individual with knowledge of another owner's device details (such as phone number and service provider) to request that device be taken out of service. This could lead to malicious acts against individuals for which the network operator may be liable.

Req. Number	Requirement
ATH-VER-0020	A request from a device owner to a network operator to disable a device must be authenticated by the network operator.

6.4.2 Authentication by Owner

In the case where the owner has direct access to a disabling tool that access could be authenticated by normal username and password credentials and would only control the device which is registered to that particular owner.

Req. Number	Requirement
ATH-VER-0030	An owner request to disable a device must be authenticated and must only control the device which is registered to that owner.

6.5 Device can only be Disabled from an Authorized Server

In a further attempt to prevent device disabling attacks against innocent mobile users 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	The mechanism to disable a mobile device must only be executed from an authorized server supporting the disable function. In order to fulfil this requirement the following is needed: • A secure connection between the device and server • Authentication by the server of the device • Authentication by the device of the server and the server being authorized to perform the function

6.6 Secure Location and Access to Servers Operating the Disabling Feature

Experience has shown that a major weakness of the SIM lock feature (which is 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.

Logs must be maintained and available that record ‘disable requests’.

Req. Number	Requirement
ATH-SER-0020	The location and access to servers supporting the disable feature must be secure.
ATH-SER-0030	Only authorized personnel with sufficient training should be allowed to access and invoke the disabling functions.
ATH-SER-0040	The server must generate and retain logs of all disable requests received.

6.7 Owner Access to the Disabling Function

It would be of universal benefit if the requirement to make service calls to network operators from device loss/theft victims could be reduced. This could be possible if owners could access and invoke a device disabling function without physical involvement from, or the need for intervention by, the network operator or device manufacturer.

In addition to the device owner being able to invoke the disablement of a device if it is misplaced, lost or stolen, a mobile network operator could also invoke the disablement of devices stolen from the distribution channel.

Req. Number	Requirement
ATH-DIS-0010	The device owner should be able to access and invoke a device disabling function via the use of self-service capabilities, without needing to involve the network operator.

ATH-DIS-0020	A device owner should not be able to re-enable a device if it was disabled by the operator.

6.8 Restore Service Function

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.

Req. Number	Requirement
ATH-RES-0010	The device must have the capability to have service re-enabled by the legitimate owner after it has been disabled. It must not be capable of being re-enabled by anyone who is not the rightful owner.

6.9 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	The owner may invoke a feature to backup all device data that belongs to the owner (personal data), to a secure network server.

6.10 Device Data Protection (Device Wipe)

In order to protect user 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 must have the ability to remotely render all device data inaccessible.
ATH-WIP-0020	The owner must have the ability to remotely wipe user data (such as pictures, videos, phonebook, emails etc.) from the device. If the user data is strongly encrypted, then wiping the encryption key from the device is sufficient.

6.11 Restore and Reload Data and Applications

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

Req. Number	Requirement
ATH-RES-0020	When restoring service to a re-enabled device that was previously disabled, the owner's backed-up data and applications must be restored to the device.

6.12 Preservation of Owner Stored Data

Owner data backed-up to the 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. The measures deployed to do this must be adequate to satisfy any applicable data retention and protection requirements.

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

6.13 Execute the Disable Function in a Timely Manner

As time is of the essence, in the case of a missing device, to protect its data and its unauthorised use, once an owner has requested their device to be disabled they can expect the function to completely execute in a matter of minutes.

Req. Number	Requirement
ATH-TIM-0010	Once an owner has requested their device to be disabled, they can expect the function to complete execution in less than 15 minutes, if the device can be successfully authenticated.

6.14 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 in a “data only” mode without a connection to a mobile operator 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. Indeed in many cases, especially where a thief wants to continue using a device in the same country, they will immediately remove the network operator’s ability to communicate with the device by simply removing the SIM before continuing to use the device by just 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 and unauthorised re-use.

Req. Number	Requirement
ATH-CON-0010	The device disable function should be operable when a device is not connected to a PLMN but is connected to the Internet.

6.15 Roamed Devices

A typical scenario is where an owner 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 network, yet the owner will call their home 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 may be advised of any additional costs to invoke the function while not on the home network.

Req. Number	Requirement
ATH-ROA-0010	For lost or stolen devices registered on a visited 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 network (roaming), the owner may be advised of any additional costs when attempting to invoke functions to back-up data, disable the device or to restore the device.

6.16 Prevention of Unauthorized Device Re-initialization

Whilst 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 should have 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 should continue to implement and evolve measures to deter and prevent the unauthorized re-initialization of a lost or stolen device to a state where it can be used by someone other than the owner. State of the art solutions from component providers should be used to achieve this critical goal.

Note: Re-initialization includes using factory reset, operating system re-install, and re-flash of the device boot loader to bypass the authorized owner credentials. Included in this requirement 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. Device re-initialization for legitimate purposes e.g. re-sale, should be available to the owner.

Req. Number	Requirement
ATH-UNA-0010	Factory reset cannot be used as a means to bypass anti-theft measures.
ATH-UNA-0020	An unauthorized user shall not be able to access the functions of, or data on, a disabled device.
ATH-UNA-0030	Device manufacturers should continue to implement and evolve measures to deter and prevent the unauthorized re-initialization of a lost or stolen device to a state where it can be used by someone other than the owner.

6.17 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 owners' possession should be made available to the owner.
ATH-HOM-0020	If set by the owner of a device, 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.

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	Manufacturer	Operator	3rd Party	Notes
6.1 Emergency Calling: **ATH-EME-0010**		X	X		
6.2 Location Features: **ATH-LOC-0010**	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 Verify the authenticity of a disablement request **ATH-VER-0010 -> 0030**	X	X	X	X	Implementation dependent
6.5 Device can only be disabled from an authorized server: **ATH-SER-0010**		X	X	X	
6.6 Secure location and access to servers operating the disabling feature: **ATH-SER-0020 -> 0040**		X	X	X	
6.7 Owner access to the disabling function: **ATH-DIS-0010 -> 0020**	X	X	X	X	Implementation Dependent
6.8 Restore service function: **ATH-RES-0010**	X	X	X	X	
6.9 Backup device data: **ATH-BAC-0010**	X	X	X	X	Depends on where and how data is stored
6.10 Device data protection (device	X	X	X	X	

wipe): **ATH-WIP-0010 -> 0020**					
6.11 Restore and reload data and applications: **ATH-RES-0020**	X	X	X	X	
6.12 Preservation of owner stored data: **ATH-STO-0010**		X	X	X	
6.13 Execute the disable function in a timely manner: **ATH-TIM-0010**		X	X	X	
6.14 Ability to disable a device when not connected to the PLMN: **ATH-CON-0010**		X		X	
6.15 Roamed devices: **ATH-VER-0010 -> 0020**	X		X		
6.16 Prevention of unauthorised device re-initialisation **ATH-UNA-0010 -> 0030**		X			
6.17 Home/lock screen display message **ATH-HOM-0010 -> 0020**	X	X	X		

Annex B Document Management

B.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
1.1	12 Dec 2014	Trnsferred PRD from SG to FASG as SG.24 v1.1	FASG	David Chong, GSMA

B.2 Other Information

Type	Description
Document Owner	FASG
Editor / Company	Nicholas Alfano, Blackberry

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.