ATIS-0700024

ATIS Standard on -

BEST PRACTICES FOR OBTAINING MOBILE DEVICE IDENTIFIERS FOR MOBILE DEVICE THEFT PREVENTION (MDTP)

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

ATIS-0700024, *Best Practices for Obtaining Mobile Device Identifiers for Mobile Device Theft Prevention (MDTP)*

Is an American National Standard developed by the **Systems and Networks (SN)** Subcommittee under the **ATIS Wireless Technologies and Systems Committee (WTSC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-0700024

ATIS Standard on

Best Practices for Obtaining Mobile Device Identifiers for Mobile Device Theft Prevention (MDTP)

Alliance for Telecommunications Industry Solutions

Approved October 2015

Abstract

This specification defines best practices for obtaining the device identifiers (e.g., International Mobile Equipment Identity [IMEI]) from mobile devices even if the mobile device is locked or disabled. This best practices specification was developed in response to Recommendation 1.5 of the December 4, 2014 Federal Communications Commission (FCC) Technological Advisory Council (TAC) report on Mobile Device Theft Prevention (MDTP).

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Wireless Technologies and Systems Committee (WTSC) develops and recommends standards and technical reports related to wireless and/or mobile services and systems, including service descriptions and wireless technologies. WTSC develops and recommends positions on related subjects under consideration in other North American, regional, and international standards bodies.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, WTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, WTSC, which was responsible for its development, had the following leadership:

M. Younge, WTSC Chair (T-Mobile)

D. Zelmer, WTSC Vice-Chair (AT&T)

P. Musgrove, WTSC SN Chair (AT&T)

G. Schumacher, WTSC SN Vice-Chair (Sprint)

D. Sennett, Technical Editor (AT&T)

The **Systems and Networks (SN)** Subcommittee was responsible for the development of this document.

Table of Contents

Table of Figures

ATIS Standard on –

Best Practices for Obtaining Mobile Device Identifiers for Mobile Device Theft Prevention (MDTP)

1 Scope, Purpose, & Application

1.1 Scope

The scope of this best practices specification on Mobile Device Theft Prevention (MDTP) is limited to phones and tablets with user interface capabilities (e.g., touchscreen) which have an International Mobile Equipment Identity (IMEI). Machine to Machine (M2M)/Internet of Things (IoT) devices and devices without cellular network capabilities (e.g., WiFi only devices) are out of scope. Personal Computers (PCs) and laptops with cellular capabilities are also out of scope.

1.2 Purpose

At the December 4, 2014 meeting, the Federal Communications Commission (FCC) Technological Advisory Council (TAC) approved the final report of the Mobile Device Theft Prevention (MDTP) working group. [Ref 1]

The MDTP working group report contains a recommendation which requires development of standards or best practices within ATIS. Specifically, Recommendation 1.5 (as quoted below) tasks industry to develop "standards, methods and procedures" to obtain device identifiers from smartphones:

> *"**Recommendation 1.5:** The FCC TAC recommends that ATIS in coordination with other appropriate industry groups (e.g., GSMA-NA Regional Interest Group) be tasked with developing standards, methods and procedures to obtain device identifiers from smartphones including those which are locked or rendered inoperable.*
>
> > *Note: Device identifiers are typically available on smartphones either through a label on the device (which may be under the back cover or under the battery), or available through a menu option on the screen. This recommendation is to define standards, methods, and procedures for obtaining such identifiers from the device even if the device is locked or disabled, and may include a combination of physical and electronic methods for obtaining the identifier.*

1.3 Application

This best practices specification is applicable to cellular network operators, to the FCC, to the FCC TAC, to mobile device manufacturers, and to third party developers of theft prevention solutions.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[Ref 1] FCC, *Report of Technological Advisory Council (TAC) Subcommittee on Mobile Device Theft Prevention (MDTP)*, Version 1.0, 4 December 2014.[1]

3 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < http://www.atis.org/glossary >.

3.1 Definitions

3.1.1 Disabled: This is the state of the mobile device after theft prevention (anti-theft) procedures have been activated. Examples of applications supporting mobile device disablement on commonly available handsets are Apple Activation Lock or BlackBerry Protect on iPhone or BlackBerry mobile devices respectively.

3.1.2 Locked: The mobile device display/keyboard/keypad does not allow access to mobile device features and applications and is password protected. To unlock the mobile device the correct password needs to be entered. This is a common feature on smartphones where the owner will set a password for the mobile device which is required to gain access to the mobile device display, keyboard, and applications. This feature normally is activated at mobile device power up, restart, and after a period of inactivity.

3.2 Acronyms & Abbreviations

ATIS	Alliance for Telecommunications Industry Solutions
CMSP	Commercial Mobile Service Provider
FCC	Federal Communications Commission
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
M2M	Machine to Machine
MDTP	Mobile Device Theft Prevention
PC	Personal Computer
TAC	Technological Advisory Council
UICC	Universal Integrated Circuit Card

[1] Available from the FCC at: < http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting12414/TAC-MDTP-Report-v1.0-FINAL-TAC-version.pdf >.

4 Assumptions

The following assumptions are associated with this best practices specification:

1. The device identifier relevant to the FCC requirement is the IMEI.
2. The mobile device has sufficient power to execute its normal boot sequence and activate the user interface.
3. The IMEI can be retrieved without knowing the authentication credentials (password, PIN, etc.) of the mobile device.
4. The IMEI is present in the mobile device.
5. A Universal Integrated Circuit Card (UICC) or equivalent may or may not be present in the mobile device.
6. A Commercial Mobile Service Provider (CMSP) may or may not have provisioned the mobile device.

5 Use Case

The primary Use Case for obtaining the device identifiers for MDTP is to support the needs of Law Enforcement. Law Enforcement personnel may encounter a mobile device during their normal execution of duties and need to determine if the mobile device has been listed as stolen on the GSMA IMEI Database[2]. Access to the IMEI is the first step in determining if a mobile device has been reported as stolen. Therefore, a quick, simple, and consistent means to obtain the IMEI from disabled, locked, or unlocked mobile devices is needed for law enforcement personnel.

> NOTE: For example, possession of stolen property could lead to an immediate arrest which is why Law Enforcement needs a quick, easy, and consistent method for obtaining the device identifier.

6 Existing Solutions

The following are some of the existing solutions for obtaining the IMEI from mobile devices:

1. The IMEI is available on some but not all mobile devices on a label attached to the mobile device which is normally located under the battery.

   > NOTE: The label can be subject to tampering. Therefore, a means to retrieve the IMEI through the user interface on the mobile device is needed.

2. From an unlocked mobile device, the IMEI can be determined by entering *#06# into the mobile phone dialer.
3. From an unlocked mobile device, the IMEI can be obtained from the mobile device configuration menus.

   > NOTE: These configuration menus vary by mobile device manufacturer and by the specific model.

4. There are no known methods for obtaining the IMEI via the user interface of a disabled or locked mobile device.

7 Best Practices for Obtaining Mobile Device IDs

The recommended best practices in this clause are based on the requirement that Law Enforcement access to the IMEI in a mobile device which is suspected of being stolen shall be achievable when the mobile device is locked or disabled, without knowing the authentication credentials (password, PIN, etc.) of the mobile device.

---

[2] Information on the GSMA IMEI Database including the general description of the database, the colored lists, the operator best practices, and access to the IMEI Database is available at: < http://www.gsma.com/managedservices/mobile-equipment-identity/the-imei-database/ >.(last visited September 10, 2015).

7.1 Mobile Device Disabled by Owner Initiated MDTP Procedures

The mobile device IMEI is a means for identifying the mobile device by its owner and whether the mobile device has been reported stolen. A mobile device retrieved by Law Enforcement may have its IMEI verified against a list of mobile devices reported as stolen. For many mobile devices the IMEI is normally located on a label under the mobile device battery, but the label can be subject to tampering and the IMEI may not be legible. Therefore it is a goal that a mobile device display the IMEI on its display screen regardless of locked or disabled status of the mobile device.

The IMEI is a 15-digit numeric string and as an example can be shown in the top left-hand corner on the mobile device display as:

Figure 7.1 – Example Display of IMEI on Mobile Device

In addition to the above, other forms of displaying the IMEI such as Code 128 barcode can aid in reading of the number and thus reduce transcription or mistakes caused by human error.

7.2 IMEI Display on Disabled or Locked Mobile Devices

For disabled or locked mobile devices, display of the device IMEI does not require specific knowledge of the mobile device user interface.

- When a mobile device is powered on, IMEI display is accomplished in two or fewer user actions (e.g., clicks/button presses, swipes, etc.).
- Clear instructions for an inexperienced user on how to obtain the IMEI are shown as well.

Examples of obtaining IMEI display from a disabled or locked mobile device could include:

- When an emergency call is initiated from a mobile device locked screen or a mobile device disabled 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.

- The IMEI can be displayed as part of the mobile device locked or mobile device disabled screen.
- There can be a “request IMEI” option on the mobile device locked or mobile device disabled screen.

7.3 IMEI Display on Unlocked Mobile Devices

For unlocked mobile devices, invoking the voice call dialer and using the numeric keypad to enter *#06# displays the IMEI.