

ICS 33.060
CCS M 36

YD

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

YD/T 2407-2013

**Technical requirements for security capability of smart mobile
terminal**

移动智能终端安全能力技术要求

(English Translation)

Issued on: April 25, 2013

Implemented on: November 1, 2013

**Issued by: Ministry of Industry and Information Technology of the People
's Republic of China 3.No action is required - F**

Table of Contents

Foreword...	3
Introduction...	4
1 Scope...	5
2 Normative references...	5
3 Terms, definitions and abbreviations...	5
4 Security capability framework and objectives of smart mobile terminal...	7
4.1 Security capability framework of smart mobile terminal...	7
4.2 Security objectives of smart mobile terminal...	7
5 Technical requirements for security capability of smart mobile terminal...	8
5.1 Basic requirements...	8
5.2 Hardware security capability requirements of smart mobile terminal...	9

Foreword

This Standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This Standard uses redrafting method to modify and adopt ITU-T X.msec-6.2012 Security aspects of smartphones, a related advice of International Telecommunication Union (ITU). It is inequivalent to ITU-T X.msec-6.

This Standard is one of the series of mobile intelligent terminal security series.

The names and structures of this series are expected to be as follows.

- a) Guidelines for the design for security capability of smart mobile terminal;
- b) YD/T 2407-2013, Technical requirements for security capability of smart mobile terminal;
- c) YD/T 2408-2013, Test methods for security capability of smart mobile terminal;
- d) YD/T 1886-2009, Security requirements and test specification for SoC in mobile terminal.

This Standard was proposed by and shall be under the jurisdiction of China Communications Standardization Association.

The drafting organizations of this Standard. Ministry of Industry and Information Technology, Beijing Spreadtrum Hi-Tech Communications Technology Co., Ltd., Datang Telecom Technology & Industry Group.

Main drafters of this Standard. Pan Juan, Kuang Xiaoxuan, Luo Hongwei, Wang Kun, Li Yunfan, Yu Lu, Yuan Guangxiang, He Guili, Shi Denian, Li Wei, Yu Huawei, Li Jianwei, Li Qian.

Introduction

With the extensive application of smart mobile terminals and the continuous expansion of functions, the security issues during the use are concerned by more and more users. In recent years, security incidents such as malicious charge, eavesdropping, theft record, location information leakage make user worry about the security of smart mobile terminals, which shall affect the development of smart mobile terminals and mobile Internet applications. The purpose of this Standard is to improve the smart mobile terminal's own security protection, to prevent a variety of security threats on smart mobile terminals, to protect users from interest damage, while preventing adverse effects on mobile communication network security caused by smart mobile terminals.

The basic principle of this Standard is that the behavior and application on smart mobile terminal shall be in line with the user's wishes. This Standard does not specify specific implementation methods and measures to facilitate innovation and development. This Standard specifies the requirements to the security capability of smart mobile terminal, from five aspects. hardware security capability requirements, operating system security capability requirements, peripheral interface security capability requirements, application software security requirements, and user data security protection

requirements. And it grades the security capability from basic security protection, difficulty of achievement, special security capability, so as to make the product has a specific quality, make it easy for consumer to choose. This Standard not only guides smart mobile terminals to preset application software more standardized and safer, but also guides smart mobile terminals to improve their own security capabilities, which shall make them perform security control on the third-party applications downloaded latter. Meanwhile, it can also prevent security impact on network caused by the preset malicious codes in smart mobile terminals.

Technical requirements for
security capability of smart mobile terminal

1 Scope

This Standard specifies the technical requirements for security capability of smart mobile terminal, including hardware security capability of smart mobile terminal, operating system security capability of smart mobile terminal, peripheral interface security capability of smart mobile terminal, application layer security requirements of smart mobile terminal, user data protection security capability of smart mobile terminal, etc. And it also grades the security capability.

This Standard is applicable to various formats of smart mobile terminals. Individual terms do not apply to special industries, professional applications. Other terminals shall also refer to use.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

YD/T 1699-2007, Information security technical specification for mobile

terminal

YD/T 1760-2012, Technical requirements for data exchange via peripheral interface of mobile terminal

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1 Smart Mobile Terminal

an open operating system capable of accessing a mobile communication network, capable of providing an application development interface, and a mobile terminal capable of installing and operating a third-party application software

3.1.2 Security Capability

technical means that can be achieved in smart mobile terminal and can prevent security threats

3.1.3 User

an object that uses smart mobile terminal's resources, including human or third-party applications

3.1.4 User Data

personal information stored on smart mobile terminal, including data generated locally by user, locally generated data for user, data coming into user data area from the outside after user's permission, etc.

3.1.5 Authorization

a process of granting user the appropriate authority according to pre-set security policy after user's identity is certified

3.1.6 Digital Signature

data attached to data unit, or data obtained by cryptographic transformation of data unit; allowing the recipient of data to verify the source and integrity of