

ICS 33.060
CCS M 36

YD

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

YD/T 2408-2013

Test methods for security capability of smart mobile terminal

移动智能终端安全能力测试方法

(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**

Table of Contents

Foreword...	3
Introduction...	4
1 Scope...	5
2 Normative references...	5
3 Terms, definitions and abbreviations...	5
4 Test methods for security capability of smart mobile terminal...	7

Foreword

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

This Standard is one of the smart mobile terminal's security series standards.

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

- a) Design guidance 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; and
- d) YD/T 1886-2009 Security requirements and test specification for system on chip in mobile terminal.

This Standard shall be used in conjunction with the Technical requirements for security capability of smart mobile terminal.

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

Drafting organizations of this Standard. China Academy of Telecommunication Research of MIIT, Spreadtrum Communications, Inc. (Beijing), and 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 and Li Xi.

Test methods for security capability
of smart mobile terminal

1 Scope

This Standard specifies the test methods for security capability of smart mobile terminal, including the test methods for security capability of smart mobile terminal's hardware, the test methods for security capability of smart mobile terminal's operator system, the test methods for security capability of smart mobile terminal's peripheral interface, the test methods for security capability of smart mobile terminal's application layer, the test methods for security capability of smart mobile terminal's user data protection, etc.

This Standard is applicable to various types of smart mobile terminal.

Individual terms do not apply to special industries and professional applications.

Other terminals shall use this Standard for reference only.

2 Normative references

The following documents are essential to the application of this document. For dated references, only the editions with the dates indicated are applicable to this document. For undated references, only the latest editions (including all the amendments) are applicable to this document.

YD/T 1886 Security requirements and test specification for system on chip
in mobile terminal

YD/T 2407-2013 Technical requirements for security capability of smart
mobile terminal

3.1 Terms and definitions

The following terms and definitions are applicable to this document.

3.1.1 Smart mobile terminal

It refers to the mobile terminal that has the ability to access a mobile communication network, an open operator system that is able to provide an application development interface, and the ability to install and run the third-party applications.

3.1.2 Security capability

It refers to the technical means that can be achieved on smart mobile terminal and are able to prevent security threats.

3.1.3 User

An object that uses the smart mobile terminal resources, including the human beings or third-party applications.

3.1.4 User data

Personal user information stored on smart mobile terminal, including the data generated locally by the users, data generated locally for the users, data entering the user data area externally after approved by the users, etc.

3.1.5 Authorization

It refers to the process of granting the user the corresponding permissions in accordance with the preset security policy, after the user identity is authenticated.

3.1.6 Digital signature

It refers to the data attached to the data unit, or the data obtained by cryptographic transformation of the data unit. Data receivers are allowed to verify the source and integrity of the data, to protect data from being tampered with and forged, and to ensure the non-repudiation of the data.

3.1.7 Code signature

It refers to a mechanism that uses a digital signature mechanism to sign all or part of a code by an entity with signature authority.

3.1.8 Operator system of smart mobile terminal

It refers to the most basic system software of smart mobile terminal, which is able to control and manage various hardware and software resources of smart mobile terminal, and to provide the interface of application development.

3.2 Abbreviations

The following abbreviations are applicable to this document.

Test item. Controlled mechanism for short message sending

Item requirements. SEE Section 5.3.1.1.3 of YD/T 2407-2013.

Preconditions. The smart mobile terminal to be tested is under normal operating condition.

Test steps.

Step 1.CHECK whether the operator system of the smart mobile terminal to be tested provides the development function of short message sending;

Step 2.If the operator system of smart mobile terminal provides the development function of short message sending, USE this function to develop a short message sending application;

Step 3.RUN this application to see whether the terminal requires the user to validate the short message sending.

Expected results.

After Step 1, if the operator system of smart mobile terminal fails to provide the development function of short message sending, this item will be evaluated as "no abnormality", and the evaluation will end;

After Step 3, if smart mobile terminal requires the user to validate, this item will be evaluated as "no abnormality", and the evaluation will end;