

---

Translated English of Chinese Standard: YDT1700-2007

Translated by: [www.ChineseStandard.net](http://www.ChineseStandard.net)

Wayne Zheng et al.

Email: [Sales@ChineseStandard.net](mailto:Sales@ChineseStandard.net)

ICS 33 60

M 36

YD

## Telecommunication Industry Standard Of the People's Republic of China

YD/T 1700-2007

---

### Testing Methods for Mobile Terminal Information Security

**YD/T 1700-2007 How to BUY & immediately GET a full-copy of this standard?**

1. [www.ChineseStandard.net](http://www.ChineseStandard.net);
2. Search --> Add to Cart --> Checkout (3-steps);
3. No action is required - Full-copy of this standard will be automatically & immediately delivered to your EMAIL address in 0~25 minutes.
4. Support: [Sales@ChineseStandard.net](mailto:Sales@ChineseStandard.net). Wayne, Sales manager

Issued on: September 29, 2006

Implemented on: January 1, 2008

---

**Issued by: Ministry of Industry Information Technology, the People's  
Republic of China**

---

## Table of Contents

<b>Preface</b> .....	3
<b>1 Scope</b> .....	4
<b>2 Quoted Standards</b> .....	4
<b>3 Definitions and Acronyms</b> .....	5
<b>3.1 Definitions</b> .....	5
<b>3.2 Acronyms</b> .....	6
<b>4 Overview</b> .....	7
<b>4.1 Test Environment</b> .....	7
<b>4.2 Terminal Information</b> .....	8
<b>4.3 Classes of Test Items</b> .....	8
<b>5 Mobile Terminal Access Security Test</b> .....	9
<b>5.1 Test of Basic Service and Functions</b> .....	9
<b>5.2 Test of Security-related Signaling Protocol</b> .....	11
<b>6 Mobile Terminal Security Test</b> .....	14
<b>6.1 User Identity Authentication</b> .....	14
<b>6.2 Mobile Terminal Hardware Security</b> .....	19
<b>6.3 Data Access Security</b> .....	21
<b>6.4 OS Security</b> .....	25
<b>7 Card Interface Test</b> .....	32
<b>7.1 GSM/GPRS Terminal SIM/ME Interface Test</b> .....	32
<b>7.2 CMA Terminal UIM/MS Interface Test</b> .....	34
<b>7.3 WCDMA Terminal Cu Interface Test</b> .....	34
<b>7.4 TD-SCDMA Terminal Cu Interface Test</b> .....	36

## Preface

This Standard is one of the serial mobile terminal information security specifications. The structure and names of the serial specifications are as follows:

1. YD/T 1699-2007 “Technical Requirements for Mobile Terminal Information Security”;
2. YD/T 1700-2007 “Testing Methods for Mobile Terminal Information Security”;

Where, YD/T1699-2007 “Technical Requirements for Mobile Terminal Information Security” is the technical basis for this Standard.

This Standard is proposed and managed by China Telecommunication Standardization Association.

This Standard is developed by: MII Telecommunication Institute, Huawei Technology, Datang Telecom Technology & Industry Group, ZTE Inc., and China Mobile Communication Corporation.

This Standard is drafted by: Pan Juan, Kuang Xiaoxuan, Zhang Xiang, Luo Hongwei, Li Jinyi, and Liujun.

---

# Testing Methods for Mobile Terminal Information Security

## 1 Scope

This Standard specifies testing methods for mobile terminal information security, including the testing methods for terminal hardware security, terminal software security, and OS application security, as well as the testing methods for mobile terminal access security and information transfer security, mobile terminal personal information confidentiality security etc.

This Standard applies to terminal equipment in the second generation mobile communication network and above. This Standard does not specify testing requirements related to EMC, EMI or electrical security.

## 2 Quoted Standards

The following standards constitute stipulations of this Standard after quoted. All the revision versions (excluding correction version) of the quoted standards specified with date are not applicable for the document. Constituents are encouraged to use the latest version of the documents. The latest version of the quoted documents without date specified is applicable for this specification.

YD/T 1215-2006	Testing Methods of 900/1800MHz TDMA Digital Cellular Mobile Telecommunication Network General Packet Radio Service (GPRS) Equipment: Mobile Stations
YD/T 1683-2007	Testing Methods for CDMA Digital Cellular Mobile Communication Network ME-UIM Card Interface;
3GPP TS 01.61	General Packet Radio Service (GPRS): GPRS Algorithm Requirements

---

3GPP TS 31.121	UICC-Terminal Interface; USIM Application Testing Specification
3GPP TS 31.124	ME Consistency Test Specification; USAT Consistency Test Specification
3GPP TS 34.123-1	UE Consistency Test Specification: Part I Protocol Consistency Test Specification
3GPP TS 51.010-1	GSM/EDGE Radio Access Network Digital Cellular Communication System (Phase 2);MS Consistency Test Specification: Part I Consistency Test Specification
3GPP TS 51.010-4	MS Consistency Test Specification: Part IV SIM Application Toolkit Consistency Test Specification
3GPP2 C.S0038-A	HRPD Air Interface Signaling Consistency Test Specification
3GPP2 C.S0043-0	cdma200 Spread Spectrum System Signaling Consistency Test Specification
ETSI TS 102 230	Smart Card; UICC-Terminal Interface; Physical, Electrical and Logical Performance Test

### 3 Definitions and Acronyms

#### 3.1 Definitions

The following definitions apply for this Standard.

##### **Subscription Identification Management**

The management process that the mobile terminal can check whether the user is legitimate to take appropriate measures at any time.

##### **Application**

File groups or programs on the telecom smart card that are used to realize services.

##### **Network Simulator**

Simulators necessary for network system environment, such as WCDMA and GSM network simulators.

##### **File**

Collection of information with logically full significance, which is identified with one

name;

**File System**

Collection of software that manages the mobile terminal software resources in the way of software in OS, managed files and data structures;

**User Authentication**

Testing process on the validity of the user identity.

**Authorization**

Process to grant the user with appropriate permission based on predefined security policy after user authentication.

**Authorized User**

User who can execute certain operation based on security strategy. It may correspond to any defined role in this Standard based on varied operation practices.

**Operation System**

The most basic system software of mobile terminal, which controls and manages various hardware and software resources of the mobile terminal and provides the interface for application development;

**Telecom Smart Card**

Telecom Smart Card is a portable and tamper resistant device that is embedded with microprocessor. It is used to store data (such as access code, user information, keys and so on) and perform security –related operations, such as authentication and encryption. Telecom smart cards are typically SIM card, USIM card and R-UIM card.

**Cu Interface**

Interface between TD-SCDMA/WCDMA terminal and USIM card.

**KI**

User authentication key used in the authentication algorithm.

**3.2 Acronyms**

The following acronyms apply to this Standard:

A-KEY	Authentication key	鉴权密钥
-------	--------------------	------

---

20	27.20	SIM presence test
21	27.21	Advice of Charge (AoC)

SAT (SIM Application Toolbox) test is performed according to the limitations and measurement methods defined in 3GPP TS 51.010-4 “MS Consistency Test Specification: Part IV SIM Application Toolkit Consistency Test Specification”. For test item, see Table 4.

Table 4 Test Items of SAT

Sequence Number	Corresponding Chapter	Item Name
1	27.22.1	Initiation of SIM application toolkit, SIM application toolbox activation ME (Profile download)
2	27.22.2	Contents of TERMINAL PROFILE Command
3	27.22.3	Services of Active SIM Command
4	27.22.4	Active SIM Command (31 commands)
5	27.22.5	Downloading data to SIM
6	27.22.6	SIM Call Control
7	27.22.7	Event Download (11 events)
8	27.22.8	MO SMS Controlled by USIM Card

For SAT, corresponding items shall be tested according to the terminal functions provided by the manufacturer.

### 7.2 CMA Terminal UIM/MS Interface Test

CDMA terminal card interface test is performed according to the limitations and measurement methods defined in YD/T1683-2007 Testing Methods for CDMA Digital Cellular Mobile Communication Network ME-UIM Card Interface. For test item, see Table 5.

Table 5 Test Items of UIM/MS Interface

Sequence Number	Corresponding Chapter	Item Name
1	6.1	MS identification
2	6.2	UIM_ID/ESN_ME selection
3	6.3	Security-related commands
4	6.11	Handover protocol test
5	6.12	Directory valuing feature
7	6.14	Use of password
8	6.15	Abbreviated Dialing Numbers (ADN)
9	6.16	Response of UI to R-UIM Status Code
10	6.17	Electrical feature test
11	6.18	Fixed Number Dialing (FND)
13	6.20	R-UIM presence test
14	6.22	Suggested Clock Cycle Index

### 7.3 WCDMA Terminal Cu Interface Test

Test of WCDMA terminal Cu interface electrical and logical features is performed according to limitations and measurement methods defined in ETSI TS 203 230 Smart Card; UICC-Terminal



---

Number	Chapter	
1	27.22.1	Initiation of SIM application toolkit, SIM application toolbox activation ME (Profile download)
2	27.22.2	Contents of TERMINAL PROFILE Command
3	27.22.3	Active SIM Maintenance Command
4	27.22.4	Active SIM Command (31 commands)
5	27.22.5	Downloading data to SIM
6	27.22.6	SIM Call Control
7	27.22.7	Event Download (15 events)
8	27.22.8	MO SMS Controlled by USIM Card
9	27.22.9	Command code processing
8	27.22.8	MO SMS Controlled by USIM Card

For USAT, its corresponding items shall be tested according to the terminal functions provided by the manufacturer.

#### 7.4 TD-SCDMA Terminal Cu Interface Test

Test methods and index requirements of TD-SCDMA terminal Cu interface shall be consistent with the test contents of WCDMA terminal Cu interface. For test items required with network simulator, replace WCDMA network simulator with TD-SCDMA network simulator.

---