

ICS 33 60
M 36



中华人民共和国通信行业标准

YD/T 1700-2007

移动终端信息安全测试方法

Testing Motheds for Mobile Terminal Information Security

2007-09-29 发布

2008-01-01 实施

中华人民共和国信息产业部 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 定义及缩略语	1
4 概述	3
4.1 测试环境	3
4.2 终端信息	3
4.3 测试项分级	4
5 移动终端接入安全测试	4
5.1 基本业务与功能测试	4
5.2 与安全相关的信令协议测试	7
6 移动终端自身安全测试	10
6.1 用户身份认证	10
6.2 移动终端硬件安全	15
6.3 数据访问的安全性	16
6.4 移动终端操作系统的安全	21
7 移动终端卡接口测试	27
7.1 GSM/GPRS终端SIM/ME接口测试	27
7.2 CDMA终端UIM/MS接口测试	28
7.3 WCDMA终端Cu接口测试	28
7.4 TD-SCDMA终端Cu接口测试	30

前 言

本标准是移动终端信息安全系列标准之一。该系列标准的结构和名称如下：

1. YD/T1699-2007《移动终端信息安全技术要求》；
2. YD/T1700-2007《移动终端信息安全测试方法》。

其中，YD/T1699-2007《移动终端信息安全技术要求》是本标准的技术依据。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：信息产业部电信研究院、华为技术有限公司、大唐电信科技产业集团、中兴通讯股份有限公司、中国移动通信集团公司

本标准主要起草人：潘 娟、匡晓烜、张 翔、落红卫、李锦仪、刘 军

移动终端信息安全测试方法

1 范围

本标准规定了移动终端设备的信息安全测试方法，包括终端硬件的安全测试方法、终端软件的安全测试方法、操作系统的应用安全测试方法等，同时也包括移动终端接入安全和信息传输安全、移动终端个人信息的保密要求等信息安全测试方法。

本标准适用于二代（包括二代）以上移动通信网的终端设备。本标准不包含EMC、EMI或电气安全等相关的测试要求。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分。然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

YD/T 1215-2006	900/1800MHz TDMA数字蜂窝移动通信网通用分组无线业务（GPRS）设备测试方法：移动台
YD/T1683-2007	CDMA数字蜂窝移动通信网移动设备（ME）与用户识别模块（UIM）间接口测试方法
3GPP TS 01.61	通用分组无线业务（GPRS）；GPRS算法要求
3GPP TS 31.121	UICC-终端接口；USIM应用测试规范
3GPP TS 31.124	ME一致性测试规范；USAT一致性测试规范
3GPP TS 34.123-1	UE一致性测试规范；第一部分：协议一致性测试规范
3GPP TS 51.010-1	GSM/EDGE无线接入网络数字蜂窝通信系统（第2阶段）；移动台（MS）一致性规范；第一部分：一致性规范
3GPP TS 51.010-4	移动台一致性规范；第四部分：SIM应用工具箱一致性测试规范
3GPP2 C.S0038-A	HRPD空中接口 信令一致性测试规范
3GPP2 C.S0043-0	cdma200扩频系统 信令一致性测试规范
ETSI TS 102 230	智能卡；UICC-终端接口；物理，电气和逻辑性能测试

3 定义及缩略语

3.1 定义

下列定义适用于本标准。

签约识别管理

指移动终端随时检查用户是否为合法用户，并采取相应措施的管理过程。

应用（Application）

指电信智能卡上用于实现业务功能的文件组或程序。

网络模拟器 (Network Simulator)

指提供测试所需网络系统环境的模拟器, 如WCDMA网络模拟器、GSM网络模拟器。

文件 (File)

文件是在逻辑上具有完整意义的信息的集合, 它有一个名称以供识别。

文件系统 (File System)

文件系统是操作系统中以文件方式管理移动终端软件资源的软件和被管理的文件和数据结构的集合。

身份认证 (User Authentication)

对用户身份标识的有效性进行验证和测试的过程。

授权 (Authorization)

在用户身份经过认证后, 根据预先设置的安全策略, 授予用户相应权限的过程。

授权用户 (Authorized User)

依据安全策略可以执行某项操作的用户。根据实际操作的不同, 可对应于本文所定义角色的任何一个。

终端操作系统 (Operating System)

是终端最基本的系统软件, 它控制和管理终端各种硬件和软件资源, 并提供应用程序开发的接口。

电信智能卡 (Telecom Smart Card)

电信智能卡是具有嵌入式微处理器, 可携带、防篡改的设备。它用于存储数据 (如: 接入码、用户信息、密钥等) 并执行安全相关的操作, 如鉴权、加密。典型的电信智能卡有SIM卡/USIM卡/R-UIM卡。

Cu接口

指TD-SCDMA/WCDMA终端与USIM卡间的接口。

KI

在鉴权算法中所使用的用户鉴权密钥。

3.2 缩略语

下列缩略语适用于本标准。

A-KEY	Authentication key	鉴权密钥
IMSI	International Mobile Subscriber Identity	国际移动用户识别号
MS	Mobile Station	移动台
ME	Mobile Equipment	移动设备
PIN1/PIN2	Personal Identity Number	用户身份识别号
R-UIM	Removable User Identity Module	可移动用户识别模块
SAT	SIM Application Toolkit	SIM应用工具箱
SIM	Subscriber Identity Module	用户身份识别模块
UICC	Universal Integrated Circuit Card	通用集成电路卡
USIM	Universal Subscriber Identity Module	通用用户身份识别模块
USAT	USIM Application Toolkit	USIM应用工具箱

4 概述

4.1 测试环境

对于移动终端接入安全的测试，其基本业务与功能部分可以利用现网进行验证性测试，如图1所示。

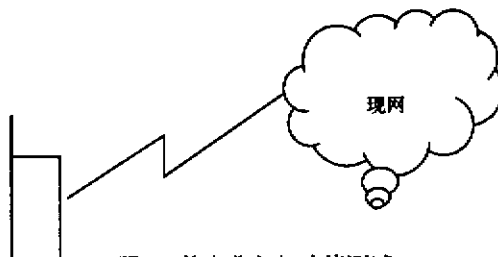


图1 基本业务与功能测试

与安全相关的信令协议测试需要借助网络模拟器来完成相关内容的测试，如图2所示。网络模拟器应满足相关标准的要求。

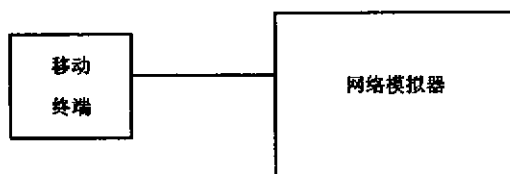


图2 与安全相关的信令协议测试

对于移动终端卡接口部分的测试，需要电信智能卡模拟器以及网络模拟器的配合来完成。测试配置如图3所示。

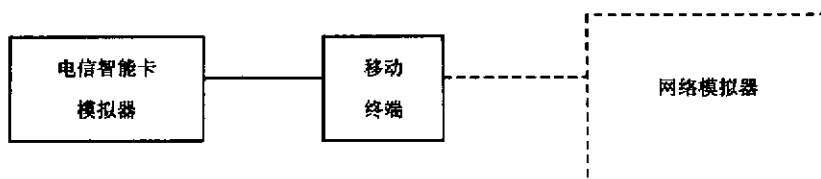


图3 移动终端卡接口测试连接图

4.2 终端信息

在测试前终端厂家需提供表1所列出的终端相关信息。

表1 终端信息

序 号	内 容
1	终端型号标识、芯片型号
2	硬件及软件平台
3	硬件及软件版本
4	IMEI 号
5	支持的口令认证方式
6	具备的外围接口
7	是否支持文件系统
8	是否具有日志
9	是否支持应用软件安装、升级和卸载
10	终端卡接口的电压类别

4.3 测试项分级

4.3.1 最低要求

表2所列测试项是所有终端必须满足的最小安全集。

表2 最小安全集所包含的测试内容

章节号	测试内容
5.1.1	紧急呼叫——功能
5.1.2	主叫号码识别显示
5.1.3	签约识别管理
5.1.4	补充业务
5.2.2	鉴权
5.2.5	紧急呼叫——协议
6.1.2	口令认证
6.3.2	电话簿访问的安全性
6.3.4	移动终端中“设置”信息访问的安全性—恢复出厂设置
6.4.2.4	IMEI号的一致性
7	移动终端卡接口测试（除智能卡主动式命令部分）

4.3.2 可选要求

对于本标准中所涉及的除表2所列测试项以外的测试内容为可选测试内容，当移动终端声称其支持相应的安全要求时，才进行相应的测试。

5 移动终端接入安全测试

5.1 基本业务与功能测试

5.1.1 紧急呼叫

测试编号：5.1.1
测试项目：紧急呼叫
测试目的：紧急呼叫是一种特殊的呼叫业务，本测试目的是验证移动终端在没有插入电信智能卡的情况下也可呼出紧急呼叫号码，紧急呼叫号码由网络定义
测试条件： 移动终端处于关机状态
测试步骤： 1. 拔出移动终端中的电信智能卡； 2. 开机； 3. 拨打普通电话号码（非紧急呼叫号码）； 4. 拨打紧急呼叫号码
预期结果： 1. 在步骤2后，移动终端应提示仅限紧急呼叫； 2. 在步骤3，移动终端应无法拨出该号码，呼叫建立失败； 3. 在步骤4，移动终端应能够正常拨打紧急呼叫号码，呼叫建立成功

5.1.2 主叫号码识别显示

测试编号：5.1.2
测试项目：主叫号码识别显示
测试目的：验证移动终端能够正确识别完整的国际有效号码
测试条件： 移动终端处于开机状态
测试步骤： 1. 在被测移动终端的电话簿中存储任意有效电话号码，并输入该号码对应的标识信息； 2. 通过在被测移动终端的电话簿中选择或输入步骤1中已存储的电话号码，并发起呼叫； 3. 通过本机号码为步骤1中已存储电话号码的移动终端向被测移动终端发起呼叫
预期结果： 1. 电话号码及其对应标识信息的存储正确有效； 2. 在发起呼叫前后，被测移动终端均应正确显示主叫号码或对应的标识信息； 3. 被测移动终端应正确显示主叫号码或对应的标识信息

5.1.3 签约识别管理

测试编号：5.1.3
测试项目：签约识别管理
测试目的：该测试仅适用于在开机状态下能够取下电信智能卡的移动终端，目的是验证移动终端能够正确进行签约识别管理
测试条件： 移动终端处于开机状态
测试步骤： 1. 使用被测移动终端进行通话，通话中取下电信智能卡； 2. 再拨打电话； 3. 进行紧急呼叫
预期结果： 1. 通话中断，移动台上应有插入电信智能卡的提示； 2. 不能拨打电话； 3. 紧急呼叫正常

5.1.4 补充业务

测试编号：5.1.4
测试项目：补充业务
测试目的：验证移动终端能够正常启用、关闭补充业务
测试条件： 使用支持补充业务的电信智能卡，移动终端处于开机状态
测试步骤： 1. 通过移动终端菜单启用以下补充业务： ● 主叫号码识别限制。 2. 使用移动终端进行拨打测试，验证该业务是否正确启用。 3. 通过移动终端菜单关闭该补充业务。 4. 使用移动终端进行拨打测试，验证该业务是否被正确关闭。 5. 对以下补充业务重复步骤1-4。 ● 无条件呼叫前转； ● 遇忙呼叫前转； ● 遇无应答呼叫前转； ● 用户不可及呼叫前转； ● 呼叫等待； ● 呼叫保持
预期结果： 1. 电话号码及其对应标识信息的存储正确有效； 2. 移动终端可以正常启用、关闭各种补充业务； 3. 在发起呼叫前后，被测移动终端均应正确显示主叫号码或对应的标识信息； 4. 被测移动终端应正确显示主叫号码或对应的标识信息

5.2 与安全相关的信令协议测试

5.2.1 概述

本节的测试主要是为了保证移动终端在信令级能够正确执行相关安全的要求，达到对用户信息的安全保护。主要内容包括鉴权、加密、信令完整性保护以及紧急呼叫。其中信令完整性保护是3G系统增强的一个安全能力，因此仅对支持信令完整性保护的终端执行该项测试。本节的紧急呼叫不同于5.1.1节，5.1.1节的紧急呼叫测试主要从功能上对移动终端执行紧急呼叫进行了验证，本节的紧急呼叫测试是从信令协议的角度对紧急呼叫的流程进行测试。

本节测试的相应信令流程请参见以下标准。

GSM/GPRS终端：

——YD/T 1215-2006《900/1800MHz TDMA数字蜂窝移动通信网通用分组无线业务（GPRS）设备测试方法：移动台》；

——3GPP TS 51.010-1《GSM/EDGE无线接入网络数字蜂窝通信系统（第2阶段）；移动台（MS）一致性规范：第一部分：一致性规范》；

——3GPP TS 01.61《通用分组无线业务（GPRS）；GPRS算法要求》。

WCDMA终端：

——3GPP TS 34.123-1《UE一致性测试规范：第一部分：协议一致性测试规范》

cdma2000终端：

——3GPP2 C.S0038-A《HRPD空中接口 信令一致性测试规范》；

——3GPP2 C.S0043-0《cdma200扩频系统 信令一致性测试规范》。

5.2.2 鉴权

测试编号：5.2.2.1
测试项目：鉴权
测试分项：鉴权接受
测试目的：验证当移动终端为网络的合法用户时，移动终端能够正确执行鉴权过程，协议流程符合标准要求
测试条件： 移动终端处于关机状态，将移动终端连接至网络模拟器，正确配置网络模拟器的相关参数（国家码、网络码等），保证移动终端能够接入网络
测试步骤： 1. 配置网络模拟器的相关鉴权参数（如：KI、A_KEY）与移动终端所使用的测试用电信智能卡一致； 2. 将测试用智能卡插入移动终端中，开机； 3. 使用被测移动终端与网络模拟器建立通话； 4. 结束通话
预期结果： 1. 在步骤2移动终端正常接入网络； 2. 在步骤3移动终端与网络模拟器正常建立通话，相关鉴权信令流程正确

测试编号：5.2.2.2
测试项目：鉴权
测试分项：鉴权拒绝
测试目的：验证当移动终端为网络的非法用户时，移动终端不能够通过鉴权认证，协议流程符合标准要求
测试条件： 移动终端处于关机状态，将移动终端连接至网络模拟器，正确配置网络模拟器的相关参数（国家码、网络码等），保证移动终端能够接入网络
测试步骤： 1. 配置网络模拟器的相关鉴权参数（如：KI、A_KEY）与移动终端所使用的测试用智能卡不一致。 2. 将测试用智能卡插入移动终端中，连接至网络模拟器，开机。 3. 使用被测移动终端与网络模拟器建立通话。 4. 结束通话
预期结果： 1. 在步骤2移动终端正常接入网络。 2. 在步骤3移动终端与网络模拟器建立通话失败，通过信令分析仪可以看到鉴权失败的消息

5.2.3 加密

测试编号：5.2.3
测试项目：加密
测试目的：验证移动终端能够正常执行加密模式，相关信令流程正确
测试条件： 移动终端关机，网络模拟器配置正确
测试步骤： 1. 正确配置网络模拟器，将测试用电信智能卡插入移动终端中，连接至网络模拟器，开机。 2. 按照网络模拟器“加密模式测试”的相应测试程序进行测试。 3. 加密模式测试主要包括：开始加密（start ciphering）、无加密（no ciphering）、旧密码（old cipher key）、模式算法和密码改变（change of mode, algorithm and key）、IMEI SV请求（IMEISV request）等5项
预期结果： 在步骤3的5项加密模式测试中，移动终端均能正确处理相应的信令流程，满足相关标准的要求，则测试通过

5.2.4 信令完整性保护

测试编号: 5.2.4
测试项目: 信令完整性保护
测试目的: 验证移动终端能够正常执行信令完整性保护, 相关信令流程正确。本测试仅适用于支持信令完整性保护的移动终端
测试条件: 移动终端关机, 网络模拟器配置正确
测试步骤: 1. 在支持完整性保护的系统中, 正确配置网络模拟器的相关参数, 使系统模拟器激活完整性保护功能。 2. 将测试用电信智能卡插入移动终端中, 连接至网络模拟器, 开机, 与网络模拟器进行与完整性保护有关的信令协议测试
预期结果: 在步骤2中, 系统模拟器正确激活完整性保护功能, 移动终端能正确处理相应信令流程, 满足相关标准的要求, 则测试通过

5.2.5 紧急呼叫

测试编号: 5.2.5
测试项目: 紧急呼叫
测试目的: 验证移动终端能够正常执行紧急呼叫, 相关信令流程正确
测试条件: 移动终端关机, 取出移动终端中的电信智能卡, 网络模拟器配置正确
测试步骤: 1. 正确配置网络模拟器的相关参数。 2. 将移动终端连接至网络模拟器, 开机。 3. 操作移动终端拨打紧急呼叫号码, 使用网络模拟器监控移动终端与网络的信令流程
预期结果: 1. 在步骤2开机后, 移动终端应提示仅限紧急呼叫。 2. 在步骤3中, 移动终端应能够正常拨打紧急呼叫号码, 相应信令流程满足相关标准的要求, 则测试通过

6 移动终端自身安全测试

6.1 用户身份认证

6.1.1 概述

本节测试目的是验证移动终端自身具备用户身份认证的能力，不涉及移动终端智能卡PIN码的验证功能，因此，配合测试所使用的智能卡应禁用PIN码的认证功能。

用户身份认证可以应用在不同的场景，本标准要求移动终端开机认证功能为必选，移动终端屏保激活身份认证为必选，以及移动终端锁卡功能为必选。因此本节的测试例将以这几种场景为基础进行测试，对于移动终端所支持的其他身份认证应用场景可以参考本节的测试例进行测试。

对于必选场景，移动终端只需支持几种认证方式中合适的一种或几种即可。

6.1.2 口令认证

测试编号：6.1.2.1
测试项目：口令认证
测试子项：开机身份认证
测试目的：验证移动终端能够正确提供对用户开机的口令身份认证
测试条件： 移动终端关机，移动终端开启了用户身份认证功能
测试步骤： 1. 将移动终端开机，移动终端提示输入用户登陆口令。 2. 输入正确的用户口令。 3. 通过移动终端的人机界面，进入用户登陆口令更改菜单。 4. 修改用户登陆口令为3位数。 5. 修改用户登录口令为4位以上数字。 6. 关机，再开机。 7. 输入旧密码。 8. 输入新密码。 9. 通过移动终端的人机界面，进入用户登录口令菜单，关闭用户身份认证功能。 10. 关机，再开机。 11. 通过移动终端的人机界面，将用户登录口令修改为正常值。 12. 关机，再开机。 13. 持续输入错误的用户口令
预期结果： 1. 步骤2后，移动终端应提示输入登陆口令正确，终端正常开机。 2. 在步骤4，移动终端应提示用户登陆口令长度过短，请求用户重新输入。 3. 在步骤5，用户登录口令成功修改。 4. 在步骤7，移动终端应提示登陆口令错误。 5. 在步骤8后，移动终端应提示输入登陆口令正确，终端正常开机。 6. 在步骤9，在关闭用户身份认证功能前，终端应提示用户输入用户登录口令，输入正确，终端应提示用户身份认证功能成功关闭。 7. 在步骤10后，移动终端开机过程应不提示用户输入用户登录口令，移动终端正常开机。 8. 在步骤13多次输入错误的用户登录口令后（根据厂家声称，但不多于5次），终端应自动采取适当措施以防止持续不断的非法攻击。如关机、锁死等

测试编号：6.1.2.2
测试项目：口令认证
测试子项：屏保激活身份认证
测试目的：验证移动终端能够正确提供对用户的屏保激活身份认证
测试条件： 移动终端关机，关闭开机用身份认证
测试步骤： <ol style="list-style-type: none"> 1. 将移动终端开机，进入屏保菜单，启用屏保激活身份认证。 2. 保持移动终端处于空闲状态。 3. 使用另一终端拨打被测终端，被测终端按接听键。 4. 呼叫结束。 5. 通过手机键盘激活系统 6. 输入错误的口令。 7. 输入正确的口令。 8. 通过菜单关闭屏保激活身份认证。 9. 输入正确的口令
预期结果： <ol style="list-style-type: none"> 1. 在步骤1，移动终端应提示输入屏保激活身份认证的口令。 2. 在步骤2，在超过等待时间后，移动终端应进入屏保状态。 3. 在步骤3，移动终端应可正常接听电话。 4. 在步骤4，呼叫结束后，移动终端应立即进入屏保状态。 5. 在步骤5，移动终端应提示用户输入屏保激活身份认证口令。 6. 在步骤6，移动终端应提示口令错误。 7. 在步骤7，移动终端应提示口令正确，移动终端被激活，进入正常使用状态。 8. 在步骤8，移动终端应提示输入口令。 9. 在步骤9，移动终端应提示屏保激活身份认证被成功关闭

6.1.3 生物特征认证

测试编号：6.1.3.1
测试项目：生物特征认证
测试子项：开机身份认证
测试目的：验证移动终端能够正确提供对用户开机的生物特征身份认证
测试条件： <ol style="list-style-type: none"> 1. 移动终端关机，移动终端开启了用户身份认证功能。 2. 本测试适用于具有生物特征认证功能的移动终端
测试步骤： <ol style="list-style-type: none"> 1. 移动终端开机。 2. 用户按照提示进行正确的生物特征认证。 3. 通过移动终端的人机界面，进入生物特征认证修改菜单。 4. 修改生物特征认证。 5. 关机，再开机。 6. 输入旧的生物特征。 7. 输入新的生物特征。 8. 通过移动终端的人机界面，关闭生物特征认证功能。 9. 关机，再开机。 10. 通过移动终端的人机界面，开启生物特征认证功能。 11. 关机，再开机。 12. 尝试多次错误的生物特征认证
预期结果： <ol style="list-style-type: none"> 1. 在步骤2后，终端应提示生物特征输入正确，终端正常开机。 2. 在步骤4，修改生物特征时，终端应首先要求输入旧的生物特征，输入正确后才可修改为新的生物特征。 3. 在步骤6，终端应提示输入错误。 4. 在步骤7后，终端应提示生物特征输入正确，终端正常开机。 5. 在步骤8，终端在关闭生物特征认证功能前应提示用户输入密码或登陆所使用的生物特征。 6. 在步骤9后，终端应不会提示输入生物特征，终端正常开机。 7. 在步骤10，终端在打开生物特征认证功能前应提示用户输入登陆所要使用的生物特征。 8. 在步骤12后，移动终端应按照厂家说明书中声明的方式对多次尝试进行相应的处理

测试编号：6.1.3.2
测试项目：生物特征认证
测试子项：屏保激活身份认证
测试目的：验证移动终端能够正确提供对用户的屏保激活身份认证
测试条件： 移动终端关机，关闭开机用身份认证
测试步骤： 1. 将移动终端开机，进入屏保菜单，启用屏保激活身份认证。 2. 保持移动终端处于空闲状态。 3. 使用另一终端拨打被测终端，被测终端按接听键。 4. 呼叫结束。 5. 通过手机键盘激活系统。 6. 输入错误的生物特征。 7. 输入正确的生物特征。 8. 通过菜单关闭屏保激活身份认证。 9. 输入正确的生物特征
预期结果： 1. 在步骤1，移动终端应提示输入屏保激活身份认证的生物特征。 2. 在步骤2，在超过等待时间后，移动终端应进入屏保状态。 3. 在步骤3，移动终端应可正常接听电话。 4. 在步骤4，呼叫结束后，移动终端应立即进入屏保状态。 5. 在步骤5，移动终端应提示用户输入屏保激活身份认证的生物特征。 6. 在步骤6，移动终端应提示输入错误。 7. 在步骤7，移动终端应提示输入正确，移动终端被激活，进入正常使用状态。 8. 在步骤8，移动终端应提示输入生物特性。 9. 在步骤9，移动终端应提示屏保激活身份认证被成功关闭

6.1.4 智能卡认证

智能卡认证对应于移动终端锁卡功能，由于电信智能卡与用户是一一对应的，通过将移动终端与电信智能卡绑定，就可以将移动终端与用户对应，从而保护合法用户信息的安全性。

测试编号：6.1.4
测试项目：智能卡认证
测试子项：移动终端锁卡功能
测试目的：验证移动终端能够正确锁定电信智能卡，防止非法用户打开移动终端读取合法用户的数据
测试条件： 移动终端关机，移动终端尚未开启锁卡功能
测试步骤： 1. 打开移动终端，通过菜单选择锁定电信智能卡。 2. 关闭移动终端，更换电信智能卡，再开机。 3. 关机，更换电信智能卡为移动终端已锁定的智能卡，再开机。 4. 通过菜单关闭智能卡锁定功能。 5. 输入错误的密码。 6. 输入正确的密码。 7. 关闭移动终端，更换电信智能卡，再开机
预期结果： 1. 在步骤1，移动终端应提示用户输入锁卡的口令。 2. 在步骤2，移动终端应提示所插入电信智能卡错误。 3. 在步骤3，移动终端正常开机。 4. 在步骤4，移动终端应提示用户输入锁卡口令。 5. 在步骤5，移动终端应提示用户输入的口令错误。 6. 在步骤6，移动终端应提示用户输入的口令正确，移动终端锁卡功能关闭。 7. 在步骤7，移动终端正常开机，正确识别电信智能卡

6.2 移动终端硬件安全

6.2.1 硬件模块的检验——开机检验

测试编号：6.2.1
测试项目：硬件模块的检验
测试子项：开机检验
测试目的：验证移动终端可在开机时进行硬件自检
测试条件： 1. 移动终端工作正常。由厂商提供一合法可替换用的硬件以及一非法可替换的硬件， 2. 如基带芯片、记录系统程序的存储器
测试步骤： 1. 将移动终端开机。 2. 将移动终端关机。 3. 移出移动终端中的某一硬件。 4. 将移动终端开机。 5. 将移动终端关机。 6. 将步骤3移出的硬件替换为另一非法的硬件（厂商提供的）。 7. 将移动终端开机。 8. 将移动终端关机。 9. 将步骤6替换的非法硬件替换为另一合法硬件（厂商提供的）。 10. 将移动终端开机
预期结果： 1. 在步骤1，移动终端应可正常开机。 2. 在步骤4、步骤7和步骤10，移动终端应采取如下安全措施中的一个或几个： ● 告警； ● 记录日志； ● 关机

6.2.2 外围接口安全控制

对于具备底部连接器、USB、红外、蓝牙、WLAN等外部接口的移动终端，当有无线连接方式（红外、蓝牙、WLAN等）请求进行数据连接时，移动终端应提示用户是否接受该无线连接。对于有线数据连接方式（底部连接器、USB等）该提示为可选要求。

测试编号：6.2.2
测试项目：外围接口安全控制
测试目的：验证当移动终端具备无线外围接口时，当以无线方式进行数据连接，移动终端会提示用户是否接受此次连接。本测试仅适用于具备红外、蓝牙、WLAN等无线外围接口的移动终端
测试条件： 移动终端工作正常
测试步骤： 1. 将被测移动终端开机。 2. 操作另一终端（具备相应无线连接方式的终端）与被测终端建立无线数据连接
预期结果： 1. 在步骤2被测移动终端应提示用户有一无线数据连接请求。 2. 用户如果选择接受，则两终端应可正常进行数据传输。 3. 用户如果选择拒绝该连接，则两终端间的无线数据连接应立即中止

6.3 数据访问的安全性

6.3.1 概述

移动终端应能够对其所存储的重要数据进行口令保护，如：电话簿（必选）、短信、证书等涉及用户隐私和安全的關鍵数据资料。本节对移动终端中六种情况的数据访问安全控制测试进行了描述，如果移动终端提供了对其他重要用户数据的访问安全控制，可以参考本节测试例的测试步骤进行相应的测试。

6.3.2 电话簿访问的安全性

测试编号：6.3.2
测试项目：电话簿访问的安全性
测试目的：验证移动终端能够提供对数据访问的安全控制
测试条件： 移动终端开机
测试步骤： 1. 通过移动终端的菜单开启电话簿密码保护功能。 2. 通过移动终端的菜单试图访问电话簿。 3. 输入错误的访问口令。 4. 输入正确的访问口令。 5. 通过移动终端的菜单关闭电话簿密码保护功能。 6. 通过移动终端的菜单访问电话簿
预期结果： 1. 在步骤2后移动终端人机界面应提示用户输入访问口令。 2. 在步骤3移动终端应提示访问口令错误。 3. 在步骤4移动终端应正确打开电话簿，用户可以正常浏览电话簿。 4. 在步骤5，关闭密码保护功能前，移动终端应提示输入密码。 5. 在步骤6移动终端应可正确访问电话簿

6.3.3 内部存储器私密区域访问的安全性

测试编号：6.3.3
测试项目：内部存储器私密区域访问的安全性
测试目的：验证移动终端能够提供对内部存储器私密区域数据访问的安全控制
测试条件： <ol style="list-style-type: none"> 1. 移动终端开机。 2. 本测试仅适用于提供了内部存储器私密区域来存储个人私密信息的移动终端
测试步骤： <ol style="list-style-type: none"> 1. 通过移动终端的菜单进入“开启用户私密区域密码保护功能”。 2. 启动“开启用户私密区域密码保护功能”。 3. 通过移动终端的菜单试图访问私密区域。 4. 输入错误的访问密码。 5. 输入正确的访问密码。 6. 通过移动终端的菜单进入“开启用户私密区域密码保护功能”。 7. 关闭用户私密区域密码保护功能。 8. 通过移动终端的菜单访问私密区域。 注：开启私密保护功能需要先输入密码，进入后设置开关功能。启动打开功能需要输入新密码 2 遍。以后访问按此新密码来验证
预期结果： <ol style="list-style-type: none"> 1. 在步骤1后，移动终端人机界面应提示用户输入访问密码。 2. 在步骤2后，移动终端人机界面应提示用户输入新密码，要求2次相同。 3. 在步骤4，移动终端应提示访问口令错误。 4. 在步骤5，移动终端应正确打开私密区域，用户可以正常浏览个人私密（有条目清单信息索引）。 5. 在步骤6后，移动终端人机界面应提示用户输入访问PIN码。 6. 在步骤7，关闭密码保护功能。 7. 在步骤8，移动终端应可正确访问私密区域

6.3.4 移动终端中“设置”信息访问的安全性

测试编号：6.3.4
测试项目：移动终端中“设置”信息访问的安全性
测试目的：验证移动终端能够提供对移动终端中设置信息访问的安全控制，其中恢复出厂设置为必选测试项
测试条件： <ol style="list-style-type: none"> 1. 移动终端开机。 2. 本测试仅适用于提供了保护防被他人篡改设置信息功能的移动终端，如恢复出厂设置、保密设置、配置设置、通话设置等
测试步骤： <ol style="list-style-type: none"> 1. 通过移动终端的菜单进入“恢复出厂设置”或“保密设置”或“配置设置”或“通话设置”。 2. 输入错误的密码。 3. 输入正确的密码
预期结果： <ol style="list-style-type: none"> 1. 在步骤2后提示密码错误。 2. 在步骤3后可以进入进行设置

6.3.5 证书访问的安全性

测试编号：6.3.5
测试项目：证书访问的安全性
测试目的：验证移动终端能够提供对证书访问的安全控制
测试条件： <ol style="list-style-type: none"> 1. 移动终端开机。 2. 本测试仅适用于提供了“证书管理”功能的移动终端
测试步骤： <ol style="list-style-type: none"> 1. 通过移动终端的菜单进入“证书管理”。 2. 查看一个证书。 3. 检查是否存在修改证书的功能。 4. 删除一个证书
预期结果： <ol style="list-style-type: none"> 1. 步骤2显示证书基本信息。 2. 步骤3终端不应该允许修改证书。 3. 步骤4移动终端应提示用户输入密码，输入成功则证书成功删除

6.3.6 系统文件访问的安全性

测试编号：6.3.6
测试项目：系统文件访问的安全性
测试目的：验证移动终端能够提供对系统文件访问的安全控制
测试条件： 1. 移动终端开机。 2. 本测试仅适用于对用户可见系统文件的移动终端
测试步骤： 1. 通过移动终端的菜单进入“文件管理”。 2. 打开系统文件目录。 3. 删除系统文件。 4. 删除系统文件目录。 5. 修改系统文件。 6. 修改系统文件目录。 7. 移动系统文件。 8. 移动系统文件目录。 9. 阅读系统文件内容
预期结果： 1. 步骤3终端不允许删除文件。 2. 步骤4终端不允许删除文件目录。 3. 步骤5终端不允许修改文件。 4. 步骤6终端不允许修改文件目录。 5. 步骤7终端不允许移动文件。 6. 步骤8终端不允许移动文件目录。 7. 步骤9终端允许阅读文件

6.3.7 不同用户访问文件的限制

测试编号：6.3.7
测试项目：不同用户访问文件的限制
测试目的：验证移动终端能够提供对不同用户访问文件进行有效控制
<p>测试条件：</p> <p>移动终端开机。</p> <ol style="list-style-type: none"> 1. 用户 X 和用户 Y 具有相应的权限。 2. 本测试仅适用于支持多用户登录以及开放文件系统功能给用户的移动终端
<p>测试步骤：</p> <ol style="list-style-type: none"> 1. 用户X通过登录移动终端的菜单进入“文件管理”。 2. 打开系统文件目录。 3. 新增2个文件A、B。将文件A修改成用户Y可修改。 4. 注销后，用户Y登录通过移动终端的菜单进入“文件管理”。 5. 打开系统文件目录。 6. 修改文件A。 7. 修改文件B。 8. 读取文件B。 9. 删除文件B
<p>预期结果：</p> <ol style="list-style-type: none"> 1. 步骤6终端可修改文件A。 2. 步骤7终端不可修改文件B。 3. 步骤8终端可读取文件B。 4. 步骤9终端不可删除文件B

6.4 移动终端操作系统的安全

6.4.1 概述

移动终端操作系统的安全包括系统软件开机一致性认证、文件系统的安全、指令系统的安全、软件管理的安全以及日志管理的安全，本节将对移动终端操作系统的安全的各个方面进行测试，以保证移动终端操作系统的安全。

6.4.2 系统软件一致性

测试编号：6.4.2.1
测试项目：系统软件一致性
测试子项：系统程序一致性检测
测试目的：如果系统程序被非授权修改，则在启动过程中，可以被检测出来
测试条件： <ol style="list-style-type: none"> 1. 由厂商提供 FLASH 中系统程序段地址范围。 2. 移动终端开机
测试步骤： <ol style="list-style-type: none"> 1. 将移动终端关机。 2. 修改FLASH程序段任何一部分。 3. 开机。 4. 关机。 5. 恢复被改动的FLASH程序段部分。 6. 开机。 7. 选择不同的FLASH地址进行修改，重复步骤1~6
预期结果： <ol style="list-style-type: none"> 1. 在步骤3，移动终端应无法正常开机。 2. 在步骤6，移动终端应可正常开机

测试编号：6.4.2.2
测试项目：系统软件一致性
测试子项：软件升级一致性检测
测试目的：如果升级程序被非授权修改，则在升级过程中，就可以被检测出来，不需要等到程序被执行
测试条件： <ol style="list-style-type: none"> 1. 移动终端开机。 2. 可以通过 USB、UART、JTAG 等有线接口或者空中无线接口进行升级
测试步骤： <ol style="list-style-type: none"> 1. 移动终端开机。 2. 通过菜单引导，进入软件升级界面。 3. 用合法软件进行升级。 4. 把合法软件修改任意一部分，进行升级
预期结果： <ol style="list-style-type: none"> 1. 在步骤3，移动终端应提示升级完成。 2. 在步骤4，移动终端应提示升级失败

测试编号：6.4.2.3
测试项目：系统软件一致性
测试子项：文件系统一致性检测
测试目的：检测 FLASH 中存放文件系统区域的一致性
测试条件： <ol style="list-style-type: none"> 1. 由厂商提供 FLASH 中文件系统区域有效地址范围。 2. 移动终端开机。 3. 本测试仅适用于提供了文件系统的移动终端
测试步骤： <ol style="list-style-type: none"> 1. 将移动终端关机。 2. 修改FLASH文件系统区域到有效地址范围之外。 3. 开机
预期结果： <p>在步骤3，移动终端开机后，应提示文件系统不一致</p>

测试编号：6.4.2.4
测试项目：系统软件一致性
测试子项：IMEI 号的一致性
测试目的：检查移动终端是否具有识别 IMEI 号遭到非法篡改的能力
测试条件： <ol style="list-style-type: none"> 1.移动终端关机。 2.由厂商提供修改 IMEI 号的方法
测试步骤： <ol style="list-style-type: none"> 1. 修改IMEI号 2. 将移动终端开机。 3. 将移动终端关机。 4. 恢复被修改的IMEI号。 5. 将移动终端开机
预期结果： <ol style="list-style-type: none"> 1. 在步骤2，移动终端应提示“IMEI号错误”，无法正常使用（关机或无法进行任何操作）。 2. 在步骤5，移动终端应正常开机

6.4.3 文件系统

测试编号：6.4.3.1
测试项目：文件系统
测试子项：文件的创建与存储
测试目的： 1. 验证移动终端操作系统的文件系统满足基本的文件管理要求。 2. 本测试仅适用于具有文件系统的移动终端
测试条件： 移动终端工作正常
测试步骤： 1. 打开移动终端，以授权用户的身份进入。 2. 创建一个新的文件，设置文件名、用户名、存取权限、文件类型、文件属性。 3. 察看该文件的属性
预期结果： 1. 在步骤2，用户可以正常设置文件的名称、用户名、存取权限、文件类型。 2. 在步骤3，应可以查看到文件建立的日期、文件最近修改日期、访问日期、文件的有效期限、文件的大小等

测试编号：6.4.3.2
测试项目：文件系统
测试子项：文件的访问安全
测试目的： 1. 验证移动终端操作系统的文件系统满足基本的文件管理要求。 2. 本测试仅适用于具有文件系统的移动终端
测试条件： 移动终端工作正常
测试步骤： 1. 打开移动终端，以授权用户的身份进入。 2. 选择某一文件，修改文件的属性：隐藏属性、系统属性、只读属性、存档属性 3. 察看该文件的属性。 4. 删除某一用户目录。 5. 删除某一系统目录
预期结果： 1. 在步骤2，用户可以修改文件的各属性。 2. 在步骤3，用户可以查看到文件的相关属性已被修改为相应的值。 3. 在步骤4，用户应可以成功删除用户目录。 4. 在步骤5，用户应不能够删除系统目录

测试编号：6.4.3.3
测试项目：文件系统
测试子项：文件管理
测试目的： 1. 验证移动终端操作系统的文件系统满足基本的文件管理要求。 2. 本测试仅适用于具有文件系统的移动终端
测试条件： 移动终端工作正常
测试步骤： 1. 打开移动终端，以授权用户的身份进入。 2. 删除某一用户目录。 3. 删除某一用户文件。 4. 更新某一用户文件，察看文件属性
预期结果： 1. 在步骤2，操作系统应向用户进行告警。 2. 在步骤3，操作系统应向用户进行告警。 3. 在步骤4，文件属性中的修改时间、访问时间应已更新为最近的时间

6.4.4 指令系统

测试编号：6.4.4
测试项目：指令系统
测试目的： 1. 验证移动终端操作系统未向未授权应用程序提供直接调用 AT 指令的公开 API 函数。 2. 本测试仅适用于为用户开放了串口等外部接口的移动终端
测试条件： 通过移动终端的外部接口将移动终端连接到电脑，通过电脑中的超级终端与移动终端建立连接。移动终端厂家提供 AT 指令的合法用户名和密码。移动终端启用 PIN 码
测试步骤： 1. 将移动终端开机。 2. 当移动终端提示用户输入PIN码时，通过超级终端输入AT指令AT^CPIN=[PIN]。 3. 在超级终端窗口内输入AT指令的合法用户名和密码。 4. 通过超级终端输入AT指令AT^CPIN=[PIN]
预期结果： 1. 在步骤2，超级终端内输入的AT命令应返回错误。 2. 在步骤4，移动终端应提示输入PIN码正确，移动终端正常开机

6.4.5 软件管理

测试编号：6.4.5.1
测试项目：软件管理
测试子项：软件安装管理
测试目的： 1. 验证移动终端操作系统能够确保应用软件安装过程的安全可靠。 2. 本测试适用于具有软件安装能力的移动终端
测试条件： 移动终端工作正常，移动终端有足够的存储空间来安装应用软件
测试步骤： 1. 下载没有提供证明软件合法性措施的软件于移动终端上。 2. 在移动终端上安装该软件
预期结果： 1. 在步骤2，移动终端操作系统应提示用户该软件为未授权软件。 2. 移动终端应采取以下措施中的一种或几种： <ul style="list-style-type: none"> ● 继续安装； ● 拒绝安装。 3. 如果用户选择了继续安装，安装成功后，该软件应不能运行

测试编号：6.4.5.2
测试项目：软件管理
测试子项：软件更新管理
测试目的： 1. 验证移动终端操作系统能够确保应用软件更新过程的安全可靠。 2. 本测试适用于具有软件安装能力的移动终端
测试条件： 移动终端工作正常，移动终端已安装应用软件
测试步骤： 1. 更新移动终端上的某一应用软件。 2. 在应用软件更新过程中，发生掉电。 3. 重新开机，运行该软件。 4. 重新进行该软件的更新
预期结果： 1. 在步骤3，应用软件应可正常运行。 2. 在步骤4，应用软件应可正常进行更新

测试编号: 6.4.5.3
测试项目: 软件管理
测试子项: 软件删除管理
测试目的: 1. 验证移动终端操作系统能够确保应用软件删除过程的安全可靠。 2. 本测试适用于具有软件安装能力的移动终端
测试条件: 移动终端工作正常, 移动终端已安装应用软件
测试步骤: 1. 在移动终端上删除某一应用软件。 2. 检查移动终端剩余空间
预期结果: 1. 在步骤1, 应用软件应可被成功删除。 2. 在步骤2, 应可查看到存储空间被释放, 剩余存储空间增加

6.4.6 日志管理

测试编号: 6.4.6
测试项目: 日志管理
测试目的: 1. 验证具有日志的移动终端, 其日志满足日志管理的基本要求。 2. 本测试仅适用于具有日志的移动终端
测试条件: 1. 移动终端关机。 2. 开启移动终端的开机用户身份认证。 3. 确认系统设定的日志文件大小
测试步骤: 1. 移动终端开机。 2. 输入错误的开机密码。 3. 输入正确的开机密码。 4. 查看移动终端操作系统日志。 5. 不断地进行开机操作, 输入两次错误的开机密码, 输入一次正确的开机密码。 6. 访问移动终端操作系统日志。 7. 输入错误的授权密码。 8. 输入正确的授权密码。 9. 察看日志文件大小, 删除日志文件
预期结果: 1. 在步骤4, 打开日志前, 操作系统应提示用户输入授权密码。打开的日志应包括以下要素: 日期、时间、事件发起者、事件类型、事件简单描述信息。 2. 在步骤6, 访问操作系统日志时, 操作系统应提示用户输入授权密码。 3. 在步骤7, 操作系统应提示用户无权访问系统日志。 4. 在步骤8, 用户应可成功访问系统日志。 5. 在步骤9, 察看到的日志文件的大小不超过系统所设定的大小, 日志保存了最新的日志内容。授权用户可以删除日志文件

6.4.7 安全服务

测试编号：6.4.7
测试项目：安全服务
测试子项：程序加载的控制管理
测试目的： 1. 验证移动终端操作系统平台能够进行程序加载的控制管理。 2. 本测试仅适用于能够加载程序的移动终端
测试条件： 移动终端剩余存储空间小于将要加载的程序 1 所需要的空间，大于将要加载的程序 2 所需要的空间
测试步骤： 1. 在移动终端上加载程序1。 2. 在移动终端上加载程序2，加载过程中发生电力不足或掉电。 3. 再次开机，检查移动终端上是否残留有未加载成功的程序2的相关目录和文件
预期结果： 1. 在步骤1，移动终端应提示用户存储空间不足，并停止程序的加载。 2. 在步骤3，应检查到移动终端中没有残留有未加载成功的程序2的相关目录和文件

7 移动终端卡接口测试

7.1 GSM/GPRS 终端 SIM/ME 接口测试

GSM/GPRS终端卡接口测试按照3GPP 51.010-1中第27章规定的限值和测量方法进行，测试项目见表3。

表3 SIM/ME 接口测试项目

序号	对应章节号	项目名称
1	27.1	MS通过短IMSI识别
2	27.2	MS通过短TMSI识别
3	27.3	MS通过长TMSI识别
4	27.4	MS通过长IMSI识别，TMSI更新和加密密钥序列号指配
5	27.5	禁止PLMN，位置更新和未定义的加密密钥
6	27.6	MS更新禁止PLMN 列表
7	27.7	MS删除禁止PLMN 列表
8	27.8	MS更新PLMN选择列表
9	27.9	MS认可PLMN选择列表的优先顺序
10	27.10	MS访问控制管理
11	27.11	交换协议测试
12	27.12	目录赋值特性
14	27.14	密码的使用
15	27.15	缩位拨号（ADN）
16	27.16	MMI对SIM状态编码的反应
17	27.17	电气性能测试
18	27.18	固定号码拨号（FND）
19	27.19	状态识别
20	27.20	SIM存在与否的检测
21	27.21	账单（AoC）

SAT（SIM应用工具箱）部分测试按照3GPP TS 51.010-4《移动台一致性规范：第四部分：SIM应用工具箱一致性测试规范》中规定的限制和测量方法进行，测试项目见表4。

表4 SAT 测试项目

序号	对应章节号	项目名称
1	27.22.1	SIM应用工具箱的初始化，SIM应用工具箱激活ME（Profile 下载）
2	27.22.2	TERMINAL PROFILE命令的内容
3	27.22.3	主动式SIM命令的服务
4	27.22.4	主动式SIM命令（31个命令）
5	27.22.5	下载数据到SIM
6	27.22.6	SIM呼叫控制
7	27.22.7	事件下载（11个事件）
8	27.22.8	SIM控制的MO短消息

SAT部分根据厂家提供的终端支持情况进行相应测试项目的测试。

7.2 CDMA 终端 UIM/MS 接口测试

CDMA终端卡接口测试按照YD/T1683-2007《CDMA数字蜂窝移动通信网移动设备（ME）与用户识别模块（UIM）间接口测试方法》中规定的限值和测量方法进行，测试项目见表5。

表5 UIM/MS 接口测试项目

序号	对应章节号	项目名称
1	6.1	MS标识
2	6.2	UIM_ID/ESN_ME的选择
3	6.3	与安全相关的命令
4	6.11	交换协议测试
5	6.12	目录赋值特性
7	6.14	密码的使用
8	6.15	缩位拨号（AND）
9	6.16	UI对R-UIM状态编码的反应
10	6.17	电气性能测试
11	6.18	固定号码拨号（FDN）
13	6.20	R-UIM存在与否的检测
14	6.22	建议的时钟周期索引

7.3 WCDMA 终端 Cu 接口测试

WCDMA终端Cu接口电气、逻辑特性测试按照ETSI TS 102 230《智能卡：UICC-终端接口：物理、电气和逻辑性能测试》中规定的限值和测量方法进行，测试项目见表6。

表6 Cu 接口电气、逻辑特性测试项目

序号	对应章节号	项目名称
1	5.1	电压转换状态测试
2	5.2	终端每一触点的电气性能测试
3	6.1	ATR
4	6.2	1.8V技术的UICC的时钟停止模式
5	6.3	3V技术的UICC的时钟停止模式
6	6.4	速率增强
7	7.1	字符传输
8	7.2	T=0协议测试
9	7.3	T=1协议测试
10	8.1	UICC存在与否的检测

WCDMA终端Cu接口SIM应用特性测试按照3GPP TS 31.121《UICC-终端接口：USIM应用测试规范》中规定的限值和测量方法进行，测试项目见表7。

表7 Cu 接口 SIM 应用特性测试项目

序号	对应章节号	项目名称
1	5.1	IMSI/TMSI的处理
2	5.2	接入控制处理
3	6.1	PIN的处理
4	6.2	固定拨号（FDN）的处理
5	6.3	禁止呼出号码（BDN）的处理
6	6.4	计费通知（AoC）的处理
7	7.1	FPLMN的处理
8	7.2	用户控制的PLMN选择器的处理
9	7.3	运营商控制的PLMN选择器的处理
10	7.4	HPLMN搜索的处理
11	8.1	电话簿程序
12	8.2	短消息处理报告

WCDMA 终端 Cu 接口 USAT 测试按照 3GPP TS 31.124《ME 一致性测试规范：USAT 一致性测试规范》中规定的限制和测量方法进行，测试项目见表 8。

表8 Cu 接口 USAT 测试项目

序号	对应章节号	项目名称
1	27.22.1	SIM应用工具箱的初始化，SIM应用工具箱激活ME（Profile下载）
2	27.22.2	TERMINAL PROFILE命令的内容
3	27.22.3	主动式SIM维护命令
4	27.22.4	主动式SIM命令（31个命令）
5	27.22.5	下载数据到SIM
6	27.22.6	SIM呼叫控制
7	27.22.7	事件下载（15个事件）
8	27.22.8	SIM控制的MO短消息
9	27.22.9	命令码的处理
8	27.22.8	SIM控制的MO短消息

USAT部分根据厂家提供的终端支持情况进行相应项目的测试。

7.4 TD-SCDMA 终端 Cu 接口测试

TD-SCDMA终端Cu接口的测试方法、指标要求与WCDMA终端Cu接口的测试内容相同，其中需要网络模拟器配合的项目，需要将WCDMA网络模拟器替换为TD-SCDMA网络模拟器。
