电 信 终 端 产 业 协 会 标 准

TAF-WG4-AS0047-V1.0.0:2019

移动智能终端安全能力测试细则

Smart Mobile Terminal Security Capability Test Manual

2019-12-26 发布　　2019-12-26 实施

电信终端产业协会　　发 布

目 次

前　　言

本标准按照 GB/T 1.1-2009给出的规则起草。

本标准由电信终端产业协会提出并归口。

本标准起草单位：中国信息通信研究院

本标准主要起草人：董雾、詹维骁、汪薇薇、魏凡星、姚一楠

引　　言

《移动智能终端安全能力》系列标准，是以移动智能终端为整体，针对终端内的硬件、操作系统和软件进行安全测试，针对YD/T 2407-2013《移动智能终端安全能力技术要求》、YD/T 2408-2013《移动智能终端安全能力测试方法》、TAF-WG4-AS0015-V1.0.0:2018《移动智能终端安全能力技术要求》、TAF-WG4-AS0016-V1.0.0:2018 《移动智能终端安全能力测试方法》要求实施检测。本标准针对标准细节进行解读，明确实施要求，内容涉及标准全部内容。

本标准适用于各种制式的移动智能终端，个别条款不适用于特殊行业、专业应用，其他终端也可参考使用。

移动智能终端安全能力测试细则

本文档就YD/T 2407-2013《移动智能终端安全能力技术要求》、YD/T 2408-2013《移动智能终端安全能力测试方法》、TAF-WG4-AS0015-V1.0.0:2018《移动智能终端安全能力技术要求》、TAF-WG4-AS0016-V1.0.0:2018《移动智能终端安全能力测试方法》标准要求制定检测细则。

1 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

YD/T 2407-2013《移动智能终端安全能力技术要求》

YD/T 2408-2013《移动智能终端安全能力测试方法》

TAF-WG4-AS0015-V1.0.0:2018《移动智能终端安全能力技术要求》

TAF-WG4-AS0016-V1.0.0:2018《移动智能终端安全能力测试方法》

2 术语、定义和缩略语

2.1 术语和定义

下列术语和定义适用于本文件。

2.1.1

移动智能终端 smart mobile terminal

具有接入移动通信网能力，能够提供应用程序开发接口的开放操作系统，并能够安装和运行应用软件的移动终端。

2.1.2

安全能力 security capability

在移动智能终端上可实现的，能够防范安全威胁的技术手段。

2.1.3

用户 user

使用移动智能终端资源的对象，包括人或第三方应用程序。

2.1.4

用户数据 user data

移动智能终端上存储的用户个人信息，包括由用户在本地生成的数据、为用户在本地生成的数据、在用户许可后由外部进入用户数据区的数据等。

2.1.5

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。

2.1.6

数字签名　digital signature

附在数据单元后面的数据，或对数据单元进行密码变换得到的数据。允许数据的接收者验证数据的来源和完整性，保护数据不被篡改、伪造，并保证数据的不可否认性。

2.1.7

代码签名　code signature

利用数字签名机制，由具有签名权限的实体对代码全部或部分功能进行签名的机制。

2.1.8

移动智能终端操作系统　operator system of smart mobile terminal

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

2.2　缩略语

下列缩略语适用于本文件。

CNNVD	中国国家信息安全漏洞库	China National Vulnerability Database of Information Security
CNVD	国家信息安全漏洞共享平台	China National Vulnerability Database
LAWMO	锁定/擦除管理对象	Lock and Wipe Management Object
NFC	近场通信	Near Field Communication
WLAN	无线局域网	Wireless Local Area Network

3　硬件安全测试细则

3.1　安全运行区域（5.2.1）

标准要求：移动终端硬件集成专用的安全运行区域，不与非安全运行区域共享存储空间，通过物理隔离防止篡改或非法获取。具备硬件实现的密码模块，实现密码算法相关功能。

测试细则：提供隔离方案设计说明文档，硬件隔离架构图。对RAM、ROM的隔离细则，提供硬件密码模块设计方案，密码模块的读写协议。

3.2　安全启动（5.2.2）

标准要求：移动智能终端安全启动代码应进行完整性验证，当验证通过后执行安全启动过程。

测试细则：提供安全启动设计文档，包括不同启动阶段的信任链构建，签名验签流程。厂商提供刷写工具，启动过程中所有涉及的二进制文件（已签名）和文件格式（HASH位置，签名位置，代码区域）。对二进制文件中HASH、签名、代码等任意修改，重新刷入，检查是否能启动。

3.3　防止物理攻击（5.2.3）

标准要求：移动智能终端密码模块应具有抵抗物理攻击能力，防止敏感信息泄漏。攻击手段包括但不限于旁路攻击和故障注入攻击。

测试细则：

（1） 密码模块抗物理攻击设计文档。提供带有密码模块的开发测试板，提供串口、GPIO接口。密码模块可通过串口进行控制，在实现加密功能时提供trigger信号。

（2） 对对称密码、非对称密码的功能进行侧信道攻击，查看密钥泄漏情况。

（3） 进行故障注入攻击，查看故障输出。

3.4 安全属性（5.2.4）

标准要求：移动智能终端运行在安全环境下，输入输出接口应配置为安全属性，且配置不可更改。

测试细则：安全外设的设计文档，安全属性如何配置管理。

3.5 根密钥生成与保护（5.2.5）

标准要求：移动智能终端安全区域根密钥应随机生成，随机数熵值应满足移动智能终端安全要求，且不低于128比特。根密钥仅在智能终端安全运行区域使用，无法被外部获取。

测试细则：提供根密钥的生成、分发和存储方式相关文档，审查根密钥管理。厂商提供根密钥随机数生成器生成的数据，进行随机性检测。

4 操作系统安全测试细则

4.1 基本能力（5.1）

标准要求：若操作系统可安装的第三方应用软件均为单一来源，且此来源内的应用软件符合标准YD/T 3228-2017《移动应用软件安全评估方法》的3级要求，则操作系统认为已经具备给用户相关提示和确认的能力。

测试细则：

（1） 单一来源：应用软件由单一厂商开发，或者经过单一厂商认证或授权。

（2） 如果单一来源内所有应用软件可满足《移动应用软件安全评估方法》标准要求，受控项判定为“未见异常”，其余项还需要按照2407,2408要求检测。

（3） 针对具备单一来源条件的移动智能终端，厂家可自行选择检测方式。

4.2 安全调用控制能力

4.2.1 通信类功能受控机制

4.2.1.1 拨打电话受控机制（5.3.1.1.1）

标准要求：应用软件调用执行拨打电话开通呼叫转移业务时，移动智能终端应明示用户业务内容，且在用户确认的情况下方可执行操作。

测试细则：

（1） 操作系统可识别呼叫转移MMI指令，系统需提示用户呼叫转移行为。

（2） 呼叫转移提示应区别于拨打电话进行单独明示。

4.2.1.2 移动通信网络数据连接（5.3.1.1.6）

标准要求：d）移动智能终端应提供数据传输控制能力，应用软件调用移动通信网络传送数据应在用户确认的情况下执行；

测试细则：

（1） 测试流程：移动智能终端恢复出厂设置，完成开机引导后，关闭WLAN开关，打开移动通信网络开关，静置测试开始；

（2） 静置测试前不主动开启应用软件，云服务等联网功能，终端完全开启后，取任意24小时检测数据作为测试结果；

（3） 开机启动过程中所产生的流量，如已经明示用户（例如在开机引导中说明），则不计算在静置流量中；如未说明则该部分流量计算在静置流量中。

（4） 本节静置检测要求与测试方法中4.5.5.8.1节相同，静置流量包含操作系统和预置应用静置流量，4.3.1.1.6.4和4.5.5.8.1两项同时进行测试，测试结果一致。

4.2.2 本地敏感功能受控机制

4.2.2.1 后台截屏功能（5.3.1.2.4）

标准要求：后台截屏是指应用软件后台运行时截取前台屏幕内容。当应用软件调用执行后台截屏时，应在用户确认的情况下才能启动截屏操作。

测试细则：截屏包括截图和录屏，终端在执行截图或录屏行为时宜有状态提示。

4.2.2.2 接收短信功能（5.3.1.2.6）

标准要求：移动智能终端应提供接收短信控制能力，应用软件调用接收短信功能应在用户确认的情况下执行。

测试细则：第三方应用接收短信则需要进行用户确认，不区分优先级，与读取短信不同。

4.2.2.3 对用户数据的操作（5.3.1.2.7）

标准要求：移动智能终端操作系统应提供对用户数据保护的功能，具体要求如下：

a）当应用软件调用对电话本数据、通话记录、短信数据、彩信数据、日程表数据进行写操作时，移动智能终端应在用户确认的情况下方可执行；

b）当应用软件需要调用对电话本数据、通话记录、上网记录、短信数据、彩信数据、日程表数据的读操作时，移动智能终端应提示用户该应用将读取这些用户数据，且在用户确认的情况下方可执行。

测试细则：

（1） 上网记录数据包括浏览记录及书签；

（2） 日程表及上网记录数据的操作要求仅针对有标准API或有其他通用调用方式的情况，第三方应用软件的私有数据如无法访问则不做要求。

4.2.3 操作系统的更新（5.3.2）

标准要求：移动智能终端应提供操作系统的更新保护功能，具体要求如下：

a）当移动智能终端提供操作系统的更新机制时，应保证执行授权的操作系统更新；

b)当移动智能终端不能保证操作系统安全的更新时,应在说明书中明示用户可能带来的安全风险；

测试细则：

（1） 终端满足a）要求，说明书中再次明示安全风险，b）项直接判定为“未见异常”；

（2） a）项进行测试时，厂商应提供相应技术支持（例：技术文档说明更新机制，安全保护等）配合验证。

4.2.4 操作系统隔离要求（5.3.3）

标准要求：预置多操作系统的移动智能终端，应采取隔离机制对多系统之间的接口和数据进行保护，防止操作系统间进行非授权通信。

测试细则：

（1） 多操作系统定义见TAF工作组文件《智能终端多操作系统或多模式研究》；

（2） 测试之前，厂商需提供材料说明多系统实现方式，隔离机制等。

（3） 原则上系统间不能进行任何通信，保证进程隔离，数据隔离；特殊场景下，厂商应提供说明并配合验证授权通信机制。

4.2.5 操作系统漏洞要求（5.3.3）

标准要求：移动智能终端操作系统应保证不含有CNVD与CNNVD6个月前公布的高危漏洞。

测试细则：

（1） 针对超危和高危漏洞进行测试，中危和低危不做要求；

（2） 测试漏洞采用抽测方式（主要为CVE漏洞），测试样本按时间递增；

（3） 漏洞发布时间与样机送测时间间隔大于等于6个月的漏洞需要检测，漏洞样本结算时间以月为单位。例：送测时间7月1日-7月31日，则检测1月及1月之前发布的漏洞；送测时间8月1日-8月30日，则检测2月及2月之前发布的漏洞；

（4） 漏洞发布时间以CNVD及CNNVD靠后时间为准，例：已知漏洞A，CNVD发布时间1月31日，CNNVD发布时间为2月1日，则漏洞发布时间为2月；

（5） 厂商可测试前提供部分说明（例：系统版本，patch版本，自证材料等），加快测试进度。

4.3 移动智能终端外围接口安全能力要求

4.3.1 无线外围接口连接状态提示（5.4.1.3）

标准要求：当移动智能终端的无线外围接口蓝牙已开启，移动终端宜在用户主界面上给用户相应的状态提示。

当移动智能终端通过无线外围接口蓝牙建立数据连接，移动智能终端应在用户主界面上给用户相应的状态提示。

当移动智能终端的无线外围接口NFC已开启，移动终端宜在用户主界面上给用户相应的状态提示。

当移动智能终端通过无线外围接口NFC建立数据连接，移动智能终端应给用户相应的提示（图标、声音或振动等）。

如果移动智能终端提供了无线外围接口的开启状态提示和数据连接状态提示，该两种状态提示应不同。

测试细则：刘海屏也需将提示在主界面显示。

4.4 移动智能终端应用层安全要求

4.4.1 应用软件安全配置能力要求（5.5.1）

标准要求：移动智能终端可提供机制对所安装的第三方应用软件的调用行为进行配置，包括对拨打电话、发起三方通话、发送短信、接收短信、发送彩信、调用移动通信网络数据连接、调用定位功能、进行通话录音、本地录音、后台截屏、拍照/摄像、访问电话本、访问通话记录、访问日程表、访问上网记录、访问短信和访问彩信的控制。

对以上调用行为进行控制至少有允许调用和禁止调用两种状态。推荐允许调用、每次调用时询问用户和禁止调用3种状态。移动智能终端应支持对以上调用行为中的3种或3种以上进行配置。对于第三方应用软件升级前后共有的调用行为，移动智能终端应保证其安全配置状态在升级前后一致。

测试细则：

（1） 第三方应用软件安全配置状态应在升级前后保持一致；

（2） 对于升级后新增的权限，默认配置不做一致性要求。

4.4.2 应用软件调用行为记录能力要求（5.5.2）

标准要求：移动智能终端应提供机制在一定时间内记录并统计第三方应用软件及预置应用软件调用行为情况，且用户可查看记录结果。移动智能终端应支持记录应用软件调用移动通信网络产生的流量数据，应用软件运行过程中最近一次调用定位功能的时间。其余应用软件调用行为记录数据应至少包括应用软件每次调用行为的起始时间，应支持记录3种或3种以上调用行为，调用行为包括拨打电话、发起三方通话、发送短信、接收短信、发送彩信、进行通话录音、本地录音、后台截屏、拍照/摄像、访问电话本、访问通话记录、访问日程表、访问上网记录、访问短信和访问彩信。

测试细则：

（1） 需记录流量数据，定位数据，及其他最少三项敏感数据；

（2） 记录敏感数据为调用情况，软件调用相应功能时记录一次；

（3） 流量数据，拨打电话、发起三方通话、发送短信、接收短信、发送彩信、进行通话录音、本地录音、后台截屏、拍照/摄像行为记录时间应不少于30天；

（4） 访问电话本、访问通话记录、访问日程表、访问上网记录、访问短信、访问彩信行为记录时间应不少于7天；

（5） 拨打电话、发起三方通话、发送短信、接收短信、发送彩信、进行通话录音、本地录音、后台截屏、拍照/摄像行为应记录调用行为起始时间，显示时间精度至少为分(min)，精度内调用行为应精确记录；

（6） 访问电话本、访问通话记录、访问日程表、访问上网记录、访问短信、访问彩信行为应记录调用行为起始时间，显示时间精度至少为分(min)，精度内调用行为可不精确记录。

（7） 记录内容应最少包括，软件名称，调用行为名称，以及调用起始时间。

4.4.3 应用软件自启动监控能力（5.5.4）

标准要求：如果移动智能终端具备第三方应用自启动程序的能力，应可以浏览和配置应用程序是否自启动。

测试细则：

（1） 包含开机自启动和后台自启动；

（2） 原则上应对所有自启动方式进行要求，例如：监听广播，服务启动等，调用方式采用抽测选择方式。

4.5 移动智能终端用户数据安全保护能力要求

4.5.1 移动智能终端的密码保护（5.6.1）

标准要求：移动智能终端密码保护功能，应满足以下安全能力要求：

a）移动智能终端应支持开机时的密码保护和开机后锁定状态下的密码保护，例如口令、图案、生物特征识别等多种形态的密码。其中，口令密码为必选的保护形式，其他形式为可选。口令认证的要求见YD/T 1699-2007 中5.5.2.1，生物特征认证的要求见YD/T 1699-2007 中5.5.2.3。

b）移动智能终端在锁定状态下，用户应不可访问系统内已存储的用户数据（至少包括电话本、短信、图片）。

测试细则：b）与U盘模式要求不同，主要针对终端侧锁屏数据查看，锁屏前产生的用户数据应不可查看，锁屏后产生的数据（例：锁屏直接进入相机拍摄的照片）不作要求。

4.5.2 文件类用户数据的授权访问（5.6.2）

标准要求：移动智能终端提供文件类用户数据的授权访问能力，当第三方应用访问被保护的用户数据时，应在用户确认的情况下才能访问。文件类用户数据包括图片、视频、音频和文档等。

测试细则：具备该保护能力即可。

4.6 操作系统其他测试细则

（1） 操作系统安全受控机制应在不影响应用正常工作的情况下运行。例：短信发送回执需正确返回给应用软件,即用户选择 “允许”需要返回短信发送成功给应用软件，用户选择“拒绝”需要返回短信发送失败给应用软件，不应影响正常计费等行为。

（2） 受控机制类要求，仅当终端支持相应功能（硬件软件支持，且有明显调用方式可供第三方应用使用）才需要系统添加对应监控机制。

（3） 操作系统某些功能不支持或接口不开放，则无需提示确认，但需要自证（文字声明等）并保留实验室验证的权利。

5 预置应用软件安全测试细则

5.1 收集用户数据（5.5.5.1）

标准要求：移动智能终端中预置的应用软件不应有未向用户明示且未经用户同意，擅自收集用户数据的行为，包括以下行为：

a）在用户无确认情况下开启通话录音、本地录音、后台截屏(N)、拍照/摄像、接收短信(N)和定位，读取用户本机号码(N)、电话本数据、通话记录、短信数据、上网记录(N)、日程表数据(N)、定位信息的行为。（对应测试方法4.5.5.1.1）

b）在用户无确认情况下读取图片、音频和视频的行为。(N)（对应测试方法4.5.5.1.2）

测试细则：

（1） 录音麦克风标志可视为明示，用户在点击后发生录音行为，视为满足标准要求。

（2） 后台截屏是指应用软件后台运行时截取前台屏幕内容，截屏包括截图和录屏操作。

（3） 打开摄像头预览即为发生拍照/摄像行为。

（4） 相机图案，二维码图案可视为拍照明示。

（5） 应用软件调用接收短信功能需向用户明示并在用户确认的情况下执行。

（6） 出现通信录的图标或者文字时，用户主动点击后发生相关行为，视为满足标准要求。

（7） 邮箱类预置应用，用户登陆账号后读取联系人，视为满足标准要求。

（8） 桌面读取联系人/短信/通话记录，视为满足标准要求。

（9） 预置应用读取短信验证码时，需要明确告知用户场景。

（10） 上网记录数据包括浏览记录及书签。

（11） 日程表及上网记录数据的操作要求仅针对有标准API或有其他通用调用方式的情况，例如将相关API开放给其他应用使用的情况。

（12） 定位类的应用通过名称实现对定位行为隐性提示：如应用名称包含天气、导航、地图，则默认为已告知用户会有定位行为，在用户主动点击应用后，无需再对定位进行单独提示。

（13） 读取图片、音频和视频的操作要求仅针对有标准API或有其他通用调用方式的情况，例如将相关API开放给其他应用使用的情况。

5.2 修改用户数据（5.5.5.2）

标准要求：移动智能终端中预置的应用软件不应有未向用户明示且未经用户同意，擅自修改用户数据的行为，包括在用户无确认情况下删除或修改用户电话本数据、通话记录、短信数据、日程表数据(N)的行为。

测试细则：日程表及上网记录数据的操作要求仅针对有标准API或有其他通用调用方式的情况，例如将相关API开放给其他应用使用的情况。

5.3 数据录入保护（5.5.5.3）

标准要求：移动智能终端中预置的支付应用软件输入认证/支付密码等敏感信息时，需采取技术措施防止密码被截获，并不得在移动智能终端界面上显示明文。（N）

测试细则：

（1） 仅针对提供支付功能的预置应用软件，如银行类，支付宝，微信等。

（2） 密码输入时不以明文方式显示。

（3） 支付密码输入建议采用专用键盘。

5.4 数据加密传输（5.5.5.4）

标准要求：移动智能终端中预置的应用软件通过公共网络传输终端上的个人信息时，应满足以下安全能力要求：

a） 预置应用软件应采用密文方式传输金融支付类，信息通信类，账户设置类，传感采集类信息；（N）（对应检测方法4.5.5.4.1）

b）预置应用软件应采用密文方式传输媒体影音类信息。 （N）（对应检测方法4.5.5.4.2）

个人信息类型定义见YD/T 3082-2016《移动智能终端上的个人信息保护技术要求》。

测试细则：

（1） 仅针对通过公共网络传输情况。

（2） 敏感数据包括但不限于用户名、密码、账户信息、传感器信息等。

5.5 组件访问控制（5.5.5.5）

标准要求：软件组件是指软件自包含的、可编程的、通过接口实现复用的软件单元。移动智能终端中预置的应用软件应对其内部包含敏感个人信息的组件及对外接口进行保护，任何未经授权的第三方应用软件不可访问或调用。（N）

测试细则：

（1） Android 操作系统的活动（activities）、服务（services）、广播接收者（broadcast receivers）、内容提供者（content providers）中exported属性的组件进行保护。

（2） 实际测试时，一是判断是否有敏感组件暴露，二是判断暴露是否合理、是否存在安全隐患。

5.6 软件认证签名（5.5.5.6）

标准要求：如果移动智能终端采用认证签名机制，在此情况下，移动智能终端预置的应用软件应包含签名信息，且签名信息真实可信。（N）

测试细则：

（1） 测试之前，对于特定操作系统，厂商需要提供查看应用签名信息的方式。

（2） 对于非谷歌官方应用，不得采用安卓公开证书 Android/emailAddress=android@android.com，也不能明显与该产品无关的签名如Android Debug等。

（3） 每一项需保证真实有效，不能为网址、乱码等无效信息。

5.7 升级更新要求（5.5.5.7）

标准要求：移动智能终端预置的应用软件更新，应在用户授权的情况下进行，当升级行为不能保证终端系统、其他应用软件、软件本身的安全时，应在说明中明示用户可能带来的安全风险。

当应用软件升级失败时，应保证应用软件能回到更新前的版本且能正常使用。

测试细则：

（1） 升级前需明示用户安全风险，并在授权下开始升级。

（2） 升级出现异常情况，可以回滚到更新前正常版本。

5.8 流量耗费（5.5.5.8.1）

标准要求：移动智能终端中预置的应用软件不应有未向用户明示且未经用户同意，擅自调用终端通信功能，造成用户流量消耗的行为，包括在用户无确认情况下通过移动通信网络数据连接、WLAN网络连接、无线外围接口传送数据的行为。

测试细则：

（1） 提供账号服务类预置应用，需要用户登陆账号后发生联网行为，视为满足标准要求。

（2） 通过名称实现对联网行为隐性提示：如应用名称包含浏览器、新闻、天气、应用商店、论坛、邮箱、云服务、钱包、支付、地图、导航，则默认为已告知用户会有联网行为，在用户点击应用后，发生联网行为，可视为满足标准要求。

（3） 门户网站：各类运营商、手机厂商的门户网站，在用户点击应用后，发生联网行为，可视为满足标准要求。

（4） 嵌入在文字中的超链接联网如果已有特殊颜色标注，用户点击后联网，可视为满足标准要求。

（5） 对于同一应用多入口的情况，需在首次进入应用时明示。例如应用有桌面入口和widget，widget行为可以在桌面入口明示。若只有widget，需要独立明示。

（6） 天气应用，桌面预置和时钟融合的widget时，天气联网和定位可在开机向导中明示，但应为可配置项，用户可关闭。

5.9 费用损失（5.5.5.8.2）

标准要求：移动智能终端中预置的应用软件不应有未向用户明示且未经用户同意，擅自调用终端通信功能，造成用户费用损失的行为，包括在用户无确认情况下拨打电话、发送短信、发送彩信、开启移动通信网络连接并收发数据的行为。

测试细则：本条目涉及行为需在每次行为发生前告知，不能仅告知一次。

5.10 信息泄露（5.5.5.8.3）

标准要求：移动智能终端中预置的应用软件不应有未向用户明示且未经用户同意，擅自调用终端通信功能，造成用户数据泄露的行为，包括以下行为：

a） 在用户无确认情况下读取并传送用户本机号码（N）、电话本数据、通话记录、短信数据、上网记录（N）、日程表数据（N）、定位信息的行为；

b）在用户无确认情况下读取并传送图片、音频和视频的行为。（N）

测试细则：

（1） 上网记录数据包括浏览记录及书签。

（2） 日程表及上网记录数据的操作要求仅针对有标准API或有其他通用调用方式的情况，例如将相关API开放给其他应用使用的情况。

（3） 定位信息为用户记录位置的相关信息。

5.11 应用软件漏洞要求（5.5.5.9）

标准要求：移动智能终端预置应用软件应保证不含有CNVD与CNNVD6个月前公布的高危漏洞。

测试细则：

（1） 只针对高危及超危漏洞进行测试，中危和低危不做要求。

（2） 测试漏洞采用抽测方式，测试样本按时间递增。

（3） 厂商可以进行自证。

5.12 测试模式要求

标准要求：移动智能终端应支持预置应用软件安全测试模式，即预置应用软件信息安全测试系统可通过该模式拦截并记录预置应用软件对操作系统的调用行为，具体行为见TAF-WG4-AS0015-V1.0.0:2018《移动智能终端安全能力技术要求》中 5.5.5 节要求。此模式仅用于配合进行测试，正式上市终端应关闭此模式。

移动智能终端预置应用软件安全测试模式应满足以下要求：

a） 终端厂商应配合提供满足测试需求的权限，或其他技术手段；

b） 终端操作系统应能够输出预置应用软件调用信息安全测试相关 API 的 log 信息。

测试细则：

（1） 移动智能终端进行测试时应具备测试模式。

（2） 测试模式需要同时满足a）和b），提供测试相关API的log信息为必要条件。

（3） 若移动智能终端部分测试项无法通过b)方法完成相应进行测试，则需终端厂商进行配合，提供满足测试需求的权限，或其他技术手段。

（4） 对终端内全部应用的敏感行为的调用日志信息进行显示，仅显示敏感行为日调用，并提供针对应用的二次筛选，可以仅显示某个或某几个应用的敏感行为日志。

（5） 日志格式，应用关键字唯一，需提供所有关键字列表。

时间 <应用中文名>[关键字] [进程名]:[函数名] 所做的操作..参数

示例1： 4 月 14 日 18:30:33 <短信>[message][com.message]:[receivedMessage] 接收短信..13812341234

（6） 敏感操作列表

序号	测试条目（操作）	类型	解读
1	开启通话录音	是	
2	本地录音	是	
3	后台截屏	是	
4	拍照/摄像	是	
5	接收短信	是	
6	定位	是	提供定位类型，如 WLAN，小区基站或 GPS
7	读取用户本机号码	是	
8	读取电话本数据	是	
9	读取通话记录	是	
10	读取短信数据	是	
11	读取彩信数据	是	
12	读取上网记录	是	
13	读取日程表数据	是	
14	读取图片（level4）	是	
15	读取视频（level4）	是	
16	读取音频（level4）	是	
17	读取定位信息	是	
18	删除电话本数据	是	
19	删除通话记录	是	
20	删除短信数据	是	
21	删除彩信数据	是	
22	删除日程表数据	是	
23	修改用户电话本数据	是	
24	修改通话记录	是	
25	修改短信数据	是	
26	修改彩信数据	是	
27	修改日程表数据	是	
28	敏感信息防截获的安全机制，及敏感信息显示规定	否	通过厂家的设计文档，确认支付类应用安全机制
29	网络传输数据信息内容(金融支付类、信息通信类、帐户设置类、传感采集类)（level3）	可选	保留操作系统差异性
30	网络传输数据信息内容(媒体影音类)（level5）	可选	保留操作系统差异性
31	组件暴露测试（level3）	可选	测试方法保留操作系统差异性
32	应用软件签名信息	可选	签名信息包含该操作系统自身提供的签名认证能力提供的信息
33	移动通信网络数据连接传送数据	是	提供 IP 信息

序号	测试条目（操作）	类型	解读
34	WLAN 网络连接传送数据	是	提供 IP 信息
35	无线外围接口传送数据	是	
36	流量耗费（静置流量）	否	
37	拨打电话	是	提供呼叫电话号码
38	发送短信	是	提供接受电话号码
39	发送彩信	是	提供接受电话号码
40	开启移动通信网络连接	是	包含开启移动数据和 WLAN 开关
41	读取并传送用户本机号码	可选	保留操作系统差异性
42	读取并传送电话本数据	可选	保留操作系统差异性
43	读取并传送通话记录	可选	保留操作系统差异性
44	读取并传送短信数据	可选	保留操作系统差异性
45	读取并传送上网记录	可选	保留操作系统差异性
46	读取并传送日程表数据	可选	保留操作系统差异性
47	读取并传送定位信息	可选	保留操作系统差异性
48	读取并传送图片（level4）	可选	保留操作系统差异性
49	读取并传送音频（level4）	可选	保留操作系统差异性
50	读取并传送视频（level4）	可选	保留操作系统差异性

5.13 预置应用其他测试细则

（1） 通过应用名称进行明示的预置应用，需要在用户主动点击应用后才可进行相关敏感行为操作。若应用自启动，用户点击应用前发生敏感行为，不符合标准要求。

（2） 只有不具备桌面图标，同时不具有应用入口的系统应用可以在开机导航中的显著位置进行明示，同时要给用户选择的权利，不能强制用户同意相关敏感行为的调用。

6 特殊行业终端测试细则

6.1 车载终端不适用情况

序号	检验项目	标准与要求	备注
1	4.6.1.1开机密码保护	移动智能终端应支持开机时的密码保护。	
2	4.6.1.2开机后锁定状态的密码保护	移动智能终端应支持开机后锁定状态下的密码保护。	

6.2 不支持安装第三方应用终端不适用情况

对于操作系统除预置应用软件外，无法安装任何第三方应用软件的移动用户终端，以下测试项不适用。

序号	检验项目	标准与要求	备注
1	4.3.1.1.1 拨打电话	应用软件调用执行拨打电话操作时，应在用户确认的情况下，拨打操作才能执行。	

序号	检验项目	标准与要求	备注
2	4.3.1.1.3 发送短信	应用软件调用执行发送短信操作时，应在用户确认的情况下，发送短信操作才能执行。	
3	4.3.1.1.4 发送彩信	应用软件调用执行发送彩信操作时，应在用户确认的情况下，发送彩信操作才能执行。	
4	4.3.1.1.6.2 移动通信网络数据连接开启、关闭的受控机制	应用软件调用开启移动通信网络数据连接功能时，应给用户相应的提示，当用户确认后连接方可开启。	
5	4.3.1.1.7.2 WLAN网络连接开启、关闭的受控机制	应用软件调用开启WLAN网络连接功能时，应给用户相应的提示，当用户确认后，连接方可开启。	
6	4.3.1.2.1.1 定位功能受控机制	应用软件调用定位功能时，移动智能终端应在用户确认的情况下才能调用。	
7	4.3.1.2.2通话录音功能启动的受控机制	当应用软件调用启动通话录音时，应在用户确认的情况下才能开启。	
8	4.3.1.2.3本地录音功能启动的受控机制	应用软件调用启动本地录音功能时，应在用户确认的情况下才能启动录音操作。	
9	4.3.1.2.4拍照/摄像功能启动的受控机制	应用软件启动拍照或摄像功能时，移动智能终端应给用户相应的提示，在用户确认的情况下方可执行拍照或摄像操作。	
10	4.3.1.2.5.5电话本数据读操作的受控机制	当应用软件需要调用对电话本数据的读操作时，该应用软件在下载、安装或首次运行时，应提示用户该应用将读取电话本数据。	
11	4.3.1.2.5.6通话记录读操作的受控机制	当应用软件需要调用对通话记录的读操作时，该应用软件在下载、安装或首次运行时，应提示用户该应用将读取通话记录数据。	
12	4.3.1.2.5.7短信数据读操作的受控机制	当应用软件需要调用对短信数据的读操作时，该应用软件在下载、安装或首次运行时，应提示用户该应用将读取短信数据。	
13	4.3.1.2.5.8彩信数据读操作的受控机制	当应用软件需要调用对彩信数据的读操作时，该应用软件在下载、安装或首次运行时，应提示用户该应用将读取彩信数据。	

序号	检验项目	标准与要求	备注
14	4.4.1.1.2蓝牙接口开启的受控机制	当应用软件调用开启蓝牙功能时，移动智能终端应给用户相应的提示，当用户确认后连接方可开启。	
15	4.4.1.1.4 NFC接口开启的受控机制	当应用软件调用开启NFC功能时，移动智能终端应给用户相应的提示，当用户确认后连接方可开启。	
16	4.5.2.1 非认证签名	如果移动智能终端支持对未经认证签名的软件下载和应用，在进行应用软件安装时，移动智能终端应能够识别应用软件的签名状态，并能够根据签名状态给用户相应的提示。	

6.3 无交互终端不适用情况

对于无用户交互方式或无操作屏幕但具有智能操作系统，且作为独立设备使用的移动用户终端，以下测试项不适用：

序号	检验项目	标准与要求	备注
1	4.3.1.1.6.1移动通信网络数据连接开启、关闭的开关	移动智能终端应提供开关可开启、关闭移动通信网络数据连接。	
2	4.3.1.1.6.3移动通信网络数据连接状态提示	当移动通信网络的数据连接处于已连接状态，移动智能终端应在用户主界面上给用户相应的状态提示。	
3	4.3.1.1.7.1 WLAN网络连接开启、关闭的开关	移动智能终端应提供开关，可开启、关闭WLAN网络连接。	
4	4.3.1.1.7.3 WLAN网络连接状态提示	当WLAN网络连接处于已连接状态，移动智能终端应在用户主界面上给用户相应的状态提示。	
5	4.3.1.2.1.2 定位功能的状态显示	应用软件调用定位功能后，移动智能终端宜在用户主界面上给用户相应的状态提示。	
6	4.4.1.1.1蓝牙接口开启/关闭开关	对于具备蓝牙功能的移动智能终端，应具备开关，可开启/关闭蓝牙。	
7	4.4.1.1.3 NFC接口开启/关闭的开关	对于具备NFC功能的移动智能终端，应具备开关，可开启/关闭NFC。	
8	4.4.1.3.1 蓝牙接口连接状态显示	当移动智能终端的蓝牙已开启，移动智能终端宜在用户主界面上给用户相应的状态提示；当移动智能终端通过蓝牙建立数据连接，移动智能终端应在用户主界面上给用户相应的状态提示。	

9	4.4.1.3.2 NFC接口连接提示	当移动智能终端的NFC已开启，移动智能终端宜在用户主界面上给用户相应的状态提示；当移动智能终端通过NFC建立数据连接，移动智能终端应给用户相应的提示（图标、声音）。	
10	4.6.1.1开机密码保护	移动智能终端应支持开机时的密码保护。	
11	4.6.1.2开机后锁定状态的密码保护	移动智能终端应支持开机后锁定状态下的密码保护。	

6.4 无输入终端不适用情况

对于无触摸屏幕、无可输入键盘、为特殊行业提供、使用过程中不存储用户个人数据且具有完善管理机制的特殊行业终端，以下测试项可不适用：

序号	检验项目	标准与要求	备注
1	4.6.1.1开机密码保护	移动智能终端应支持开机时的密码保护。	
2	4.6.1.2开机后锁定状态的密码保护	移动智能终端应支持开机后锁定状态下的密码保护。	

6.5 纯网络终端不适用情况

对于为特殊行业提供，在使用过程中需要全程联网且需要联网才可以实现其基本功能的特殊行业终端，以下测试项可不适用：

序号	检验项目	标准与要求	备注
1	4.3.1.1.6.1移动通信网络数据连接开启、关闭的开关	移动智能终端应提供开关可开启、关闭移动通信网络数据连接。	

6.6 纯 NFC 支付终端不适用情况

对于为特殊行业提供，将NFC作为主要支付手段的支付类终端，以下测试项可不适用：

序号	检验项目	标准与要求	备注
1	4.4.1.1.3 NFC接口开启/关闭的开关	对于具备NFC功能的移动智能终端，应具备开关，可开启/关闭NFC。	

附 录 A
（规范性附录）
标准修订历史

修订时间	修订后版本号	修订内容

附 录 B
（资料性附录）
附录

参 考 文 献