ICS 33.050
CCS M 30

团　体　标　准

T/TAF 047—2022
代替 T/TAF 047—2019

移动智能终端安全能力测试细则

Smart mobile terminal security capability test manual

2022-09-15 发布　　2022-09-15 实施

电信终端产业协会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替T/TAF 047-2019《移动智能终端安全能力测试细则》，与T/TAF 047-2019相比，除结构调整和编辑性改动外，主要的技术变化如下：

a) 增加了“基本能力”（见5）；
b) 增加了“安全处理单元”（见6.6）；
c) 更改了“总体要求”（见7.1，2019版的4.1）；
d) 更改了“安全调用控制能力”的内容（见7.2,2019版的4.2）；
e) 增加了“操作系统的更新”（见7.3）；
f) 增加了“多操作系统要求”（见7.4）；
g) 增加了“操作系统漏洞要求”（见7.5）；
h) 增加了“操作系统个人信息和敏感行为要求”（见7.6）；
i) 更改了“无线外围接口安全能力要求”（见8.1，2019版的4.3）；
j) 修改了“应用软件调用行为记录能力要求”（见9.1，2019版的4.4）；
k) 增加了“总体要求”（见10.1），增加了“个人信息保护”（见10.2）；
l) 更改了“收集用户数据”的内容（见10.3，2019版的5.2）；
m) 更改了“数据加密传输”的内容（见10.5，2019版的5.4）；
n) 更改了“应用软件签名”的内容（见10.6，2019版的5.6）；
o) 更改了“升级更新要求”的内容（见10.7，2019版的5.7）；
p) 更改了“费用损失”的内容（见10.8.2，2019版的5.9）；
q) 更改了“信息泄露”的内容（见10.8.3，2019版的5.10）；
r) 更改了“应用软件漏洞”的内容（见10.9，2019版的5.11）；
s) 更改了“测试模式”的内容（见10.9，2019版的5.12）；
t) 删除了“预置应用其他测试细则”（见2019版的5.13）；
u) 删除了“特殊行业终端测试细则”（见2019版的6）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、博鼎实华（北京）技术有限公司、荣耀终端有限公司、华为技术有限公司、OPPO广东移动通信有限公司、维沃移动通信有限公司、北京三星通信技术研究有限公司、北京奇虎科技有限公司、郑州信大捷安信息技术股份有限公司。

本文件主要起草人：董霁、詹维骁、汪薇薇、傅山、魏凡星、刘陶、王嘉义、赵晓娜、张琪、衣强、张悦、李腾、贾科、张玮、吴越、姚一楠、刘献伦。

本文件及其代替文件的历史版本发布情况为：

——2019年首次发布为T/TAF 047-2019；

——本次为第一次修订。

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，针对硬件安全能力、操作系统安全能力、外围接口安全能力、应用层安全、用户数据安全保护能力进行测试，针对YD/T 2407《移动智能终端安全能力技术要求》、YD/T 2408《移动智能终端安全能力测试方法》要求实施检测。本文件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。

本文件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

1 范围

本文件规定了 YD/T 2407-2021《移动智能终端安全能力技术要求》、YD/T 2408-2021《移动智能终端安全能力测试方法》标准要求对应的检测细则。

本文件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。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 2407-2021 移动智能终端安全能力技术要求

YD/T 2408-2021 移动智能终端安全能力测试方法

YD/T 3228-2017 移动应用软件安全评估方法

3 术语和定义

3.1

移动智能终端 smart mobile terminal

能够接入移动通信网，具有能够提供应用软件开发接口的操作系统，具有安装、加载和运行应用软件能力的终端。

3.2

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。

3.3

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软件。

3.4

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。

3.5

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。

3.6

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。

3.7

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。

3.8

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

运行在移动智能终端上的系统软件，控制、管理移动智能终端上的硬件和软件，提供用户操作界面、应用软件编程接口和其他系统服务的应用软件。

3.9

移动智能终端应用软件　smart mobile terminal application

移动智能终端内，能够利用移动智能终端操作系统提供的开发接口，实现某项或某几项特定任务的计算机软件或者代码片段。包含移动智能终端预置应用软件，以及互联网信息服务提供者提供的可以通过网站、应用商店等移动应用分发平台下载、安装、升级的应用软件。

3.10

移动智能终端预置应用软件　smart mobile terminal pre-installed application

移动智能终端内，在主屏幕和辅助屏界面（不包含进入界面后，通过菜单进入或者调起的功能）有用户交互入口并且可独立使用的移动智能终端应用软件。

3.11

恶意吸费　malicious charge

在用户不知情或未授权的情况下由终端上应用软件造成的用户经济损失。

3.12

框架型操作系统　Frame-based Operating System

框架型操作系统是指在移动智能终端或应用软件上，提供控制和管理应用软件的能力，并为在其上运行的应用软件提供相应开发接口的框架，主要形态有桌面型框架操作系统和应用型框架操作系统。

3.13

移动智能终端免安装应用程序 Non-installed Applications of Smart Mobile Terminal

在移动智能终端或框架型操作系统上，能够利用操作系统提供的开发接口，实现某项或某几项特定任务的应用程序，无安装过程。

4 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）

NFC：近场通信（Near Field Communication）

WLAN：无线局域网（Wireless Local Area Network）

5 基本能力

5.1 提示

标准要求：给用户的提示和明示可以是图标、文字、语音或其他明显的提示方式，对于用户主动设置为允许或主动触发的操作，认为是在用户知情的情况下执行的操作。在操作执行期间，提示应足够引起用户的注意，且提示信息应易于用户理解。

测试细则：

a) 标准中无特殊说明的情况下，提示信息用户应可直接获得，无需二次点击或其他操作(如点击链接，下拉等）即可获取相应提示内容；

b) 对于用户主动设置为允许或主动触发的操作等同于实施明示和告知；

c) 本文件内容中的明示和提示仅适用于本文件相关内容，个人信息相关明示要求应符合其他相应法律法规。

5.2 确认

标准要求：用户确认应使用户有选择的权利，即用户应能确认也能取消。

测试细则：针对第三方应用取消需包含提示时取消和事后取消。针对首次确认，一定时间内有效和长期有效的确认，需支持用户对该行为的配置能力。

5.3 开关要求

标准要求：对于移动通信网络连接、无线局域网络连接、无线外围接口的开启操作需具备任何情况下都应给用户提示并经用户确认的能力。

测试细则：针对标准要求的开关受控操作，应在提示和配置能力包含每次提示的选项。如果终端设备仅支持每次提示，则无需包含单独的配置能力。

5.4 单一来源

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：

a) 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；

b) 如果单一来源内所有应用软件可满足YD/T 3228-2017 《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YD/T 3228-2017《移动应用软件安全评估方法要求检测》、YD/T 2408-2021《移动智能终端安全能力测试方法》相关要求进行检测；

c) 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。

6 硬件安全测试细则

6.1 安全运行区域

标准要求：移动智能终端硬件集成专用的安全运行区域，安全运行区域有专享的存储空间、该存储空间不与非安全运行区域共享，通过硬件隔离防止篡改或非法获取。

测试细则：提供隔离方案设计说明文档，硬件隔离架构图。对厂商提供的技术文档进行审查，审查RAM、ROM、Flash的隔离机制，保证安全运行区域与非安全运行区域使用的存储空间是隔离的。在厂家配合下尝试在非安全运行区域对安全运行区域地址的数据进行读写或修改操作。

6.2 安全启动

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。

6.3 防止物理攻击

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。攻击手段包括旁路攻击和故障注入攻击等。

测试细则：

a) 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；

b) 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；

c) 进行故障注入攻击，查看故障输出。

6.4 安全属性

标准要求：移动智能终端运行在安全环境下，敏感输入输出接口或敏感参数应具有安全属性，其配置不可更改或仅可进行授权更改。

测试细则：

a) 厂家提供安全外设的设计文档，说明安全属性如何配置管理；
b) 安全环境下使用的敏感输入输出接口或敏感参数应配置为安全属性，且配置不可被非安全环境更改。

6.5 根密钥生成与保护

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。根密钥仅在移动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。

6.6 安全处理单元

标准要求：移动智能终端硬件集成专用安全处理单元，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：厂商提供硬件系统结构图和安全处理单元的型号，记录安全处理单元的唯一标识符。审查通信接口和密码模块接口，在厂家配合下尝试遍历密码模块的API。

7 操作系统测试细则

7.1 总体要求

操作系统测试系统总体要求如下：

a) 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；
b) 受控机制类要求，当终端不支持相应开发功能(硬件软件支持，且有明显调用方式可供第三方应用使用）时，需要自证（文字声明等）并保留实验室验证的权利；
c) 操作系统某些功能不支持或接口不开放时，需要自证（文字声明等）并保留实验室验证的权利；
d) 主界面的状态提示指在状态栏（如主屏、锁屏及下拉屏等界面的状态栏）的状态提示，状态提示与蜂窝网络信号强度和归属运营商名称显示于同一界面；
e) 屏幕较小设备可通过下拉方式在辅助屏中显示（如手表）。

7.2 安全调用控制能力

7.2.1 通信类功能受控机制

7.2.1.1 拨打电话

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，移动智能终端应提示用户业务内容，且在用户确认的情况下方可执行操作。

测试细则：

a) 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；
b) 呼叫转移提示应区别于拨打电话进行单独明示，不应在确认拨打电话操作时同时确认呼叫转移；

c） 每次开通呼叫转移业务时，应提示用户呼叫转移业务内容，宜包含呼叫转移号码，呼叫转移方式等信息。

7.2.1.2 移动通信网络数据连接

标准要求：移动智能终端通信网络数据连接，应满足以下安全能力要求：

标准原文a） 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。

标准原文c） 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。

测试细则：

a） 移动通信网络开关开启或关闭不应影响终端正常使用基本通信功能（收发短信和接打电话等）；

b） 移动网络连接状态应区别且独立于通信功能信号状态。

7.2.2 本地敏感功能受控机制

7.2.2.1 后台截屏/录屏功能

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

测试细则：

a） 若截屏和录屏为同一接口，可统一配置提示；

b） 终端在执行录屏行为时宜有状态提示。

7.2.2.2 拍照/摄像功能

标准要求：对于具备摄像头的移动智能终端，当应用软件启动摄像头功能时，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/摄像等操作。

测试细则：拍照/摄像功能指打开摄像头的操作。

7.2.2.3 接收短信功能

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。

7.2.2.4 对用户数据的操作

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、媒体影音数据（如照片、视频和音频），生物特征识别信息（如指纹识别、人脸识别等）、设备唯一可识别信息（如不可重置的设备标识符）、应用软件列表的读操作时，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；

b） 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、日程表数据进行修改（包含写和删除）操作时，移动智能终端应在用户确认的情况下方可执行；

c） 移动智能终端操作系统应支持对设备唯一可识别信息（如不可重置的设备标识符）进行去标识化保护能力。

测试细则：

a） 上网记录数据包括浏览记录及书签，原则上不包含用户主动点击加载新网页的行为；

b） 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；

c） 本文件生物特征识别信息（如指纹识别、人脸识别等）指对处于任何处理阶段的生物特征样本、生物特征参考、生物特征项或生物特性的通称。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；

d） 本文件设备唯一标识信息主要指不可重置的设备标识符，如IMEI、MAC（WLAN的固定MAC地址），该受控机制不应用Read Phone State代替；

e） 不能用“存储”替代应用对“媒体影音数据（如照片、视频和音频）”的用户数据操作提示；

f） 本文件中应用软件列表读操作受控机制，用户选择拒绝后，仅可返回空值或者调用应用自身信息。

7.3 操作系统的更新

标准要求：

a） 当移动智能终端提供操作系统的更新机制（包含系统、驱动和系统服务的安装更新）时，应在执行更新安装操作前提示用户，并在用户确认后执行相关操作；

b） 当移动智能终端提供自动更新功能时，应提供操作系统自动更新开关，且自动更新功能不应默认开启；

c）移动智能终端应提供操作系统更新包下载可控机制。如无相关机制，则移动智能终端应具备未安装的操作系统更新包的删除能力；

d） 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；

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

测试细则：

a） a,c)操作系统升级包含更新包下载和执行更新安装两个行为，两个行为可同时受控或者分开受控均符合要求，但要明确告知用户此行为包含下载和执行；

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

c） d）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。

7.4 多操作系统要求

7.4.1 多操作系统隔离要求

标准要求：如移动智能终端预置多个独立操作系统，可分别调用系统资源，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：

a） 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；

b） 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。

7.4.2 框架型操作系统安全要求

标准要求：框架型操作系统是指在移动智能终端或应用软件上，提供控制和管理应用软件的能力，并为在其上运行的应用软件提供相应开发接口的框架，主要形态有桌面型框架操作系统和应用型框架操作系统。本节仅适用于桌面型框架操作系统。桌面型框架操作系统应具备独立的操作系统安全能力，包括但不限于5.3内要求。

测试细则：若用户交互的系统桌面属于框架型操作系统桌面，其上运行的多为免安装应用，则该框架型操作系统属于桌面型框架操作系统。

7.5 操作系统漏洞要求

标准要求：保证不含有当前操作系统版本发布日期6个月前CNVD与CNNVD发布的高危及以上漏洞。

测试细则：

a) 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；

b) 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；

c) 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。

7.6 操作系统个人信息和敏感行为要求

7.6.1 操作系统个人信息保护要求

标准要求：移动智能终端操作系统不应存在未明确告知收集使用个人信息的目的、方式和范围，并获得用户同意前，读取并传送用户个人信息的行为，以及采集和读取生物特征识别信息的行为。

测试细则：在用户个人信息收集、使用规则中说明读取并传送个人信息的情况，本节 “读取并发送”指发送至服务器的个人信息。

7.6.2 操作系统敏感行为安全要求

标准要求：移动智能终端操作系统中，可安装的系统组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，以及擅自收集或泄露用户个人信息的行为。

测试细则：可安装的系统组件为非移动智能终端预置应用软件的预置程序。例如Android为Apk文件，Windows为Exe文件，iOS的Ipa文件等。

8 移动智能终端外围接口安全能力要求

8.1 无线外围接口安全能力要求

8.1.1 无线外围接口连接状态提示

标准要求：

a) 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。

b) 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。

c) 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。

d) 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）。

e) 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，则两种状态提示应不同。

测试细则：

a) 屏幕较小设备可通过下拉方式显示状态（如手表）；

b) 可穿戴设备或车载设备和主设备（手机）配对后如果存在实时数据传输，应符合相应状态要求；

c) 本节仅针对主设备数据传输至被传输设备中执行存储等相关操作的情况。

9 移动智能终端应用层安全要求（不含预置应用软件安全要求）

9.1 应用软件调用行为记录能力要求

标准要求：移动智能终端应支持记录并统计应用软件调用行为，且用户可查看记录结果：

a) 移动智能终端应支持记录非自研预置应用软件和第三方应用软件调用移动通信网络产生的流量数据，和敏感信息的调用行为，包括定位、拍照/摄像、后台截屏/录屏、通话录音、本地录音、读取短信、读取电话本、读取媒体影音数据（如照片、视频和音频），读取生物特征识别信息（如指纹识别、人脸识别等）、读取设备唯一可识别信息（如不可重置的设备标识符）的调用行为；

b) 移动智能终端应支持记录非自研预置应用软件和第三方应用软件拨打电话、发起三方通话、发送短信、接收短信、发送彩信、读取传感器信息、读取彩信、读取通话记录、读取日程表、读取上网记录、读取应用软件列表、修改短信、修改彩信、修改电话本、修改通话记录、修改日程表、修改上网记录的调用行为。

测试细则：

a) 调用移动通信网络按总额统计类型调用行为的展示：展示内容至少可查看周期内累计总额，展示形式包含应用软件名称、调用行为名称、数据总额。数据总额可持续累计或周期性累计（如每周、每月等）。当流量达到kb、Mb时可以以kb、Mb为单位进行记录；

b) 按次统计类型调用行为的展示：展示内容至少为保存期限内最后一次详情或每次详情，其中应包含应用软件名称、调用行为名称、调用行为起始时间（展示时间精度至少为分钟），可增加调用结果（允许或拒绝）等每次发生的详情；

c) 移动智能终端应保证对APP调用行为展示的公平、公正和无歧视性。如果是移动智能终端或APP不支持的调用行为，可不做展示。表1为保存和展示的基本要求示例；

d) 针对Android操作系统，通话录音行为记录，6.0以上可与本地录音合并，但需要明确是录音，但6.0以下需区分，Voice_call和Voice_mic；

e) 读取短信和读取彩信可以合并记录行为，但需明确是合并记录；

f) 因测试时长有限，检测时至少调用3次，并查看调用记录。

保存和展示的基本要求见表1。

表 1　保存和展示的基本要求

调用行为名称	保存期限	保存要求	基本展示要求
调用移动通信网络	当前自然月天数	有新增就保存	周期内累计总额

表 1　保存和展示的基本要求 （续）

调用行为名称	保存期限	保存要求	基本展示要求
获取定位	最近7天内	7 天内最近一次详情	7天内最近一次详情
拍照/摄像	最近7天	每次详情	每次详情
后台截屏/录屏	最近7天	每次详情	每次详情
通话录音	最近7天	每次详情	每次详情
本地录音	最近7天	每次详情	每次详情
读取短信	最近7天	每次详情	每次详情
读取电话本	最近7天	每次详情	每次详情
读取媒体影音数据（如照片、视频和音频）	最近7天内	7 天内最近一次详情	7天内最近一次详情
读取生物特征数据（如指纹识别、人脸识别等）	最近7天	每次详情	每次详情
读取设备唯一可识别信息（IMEI和设备MAC地址）	最近7天	每次详情	每次详情
拨打电话	最近7天	每次详情	每次详情
发起三方通话	最近7天	每次详情	每次详情
发送短信	最近7天	每次详情	每次详情
接收短信	最近7天	每次详情	每次详情
发送彩信	最近7天	每次详情	每次详情
读取传感器信息	最近7天	每次详情	每次详情
读取彩信	最近7天	每次详情	每次详情
读取通话记录	最近7天	每次详情	每次详情
读取日程表	最近7天	每次详情	每次详情
读取上网记录	最近7天	每次详情	每次详情
读取应用软件列表	最近7天	每次详情	每次详情
写删短信	最近7天	每次详情	每次详情
写删彩信	最近7天	每次详情	每次详情
写删电话本	最近7天	每次详情	每次详情
写删通话记录	最近7天	每次详情	每次详情
写删日程表	最近7天	每次详情	每次详情
写删上网记录	最近7天	每次详情	每次详情

9.2　应用软件自启动监控能力

标准要求：如果移动智能终端具备第三方应用自启动软件的能力，应可以浏览和配置应用软件是否自启动。

测试细则：

a)　包含开机自启动和关联启动；

b)　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。

10 预置应用软件安全测试细则

10.1 总体要求

应用软件安全测试细则的总体要求如下：

a) 因终端运行需要开机自启的应用可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；

b) 运行于桌面型框架操作系统上的免安装应用应满足预置应用软件安全要求；

c) 预置应用软件应由应用自身明示具体的敏感行为，不得以操作系统提供的“权限”管控机制，代替具体敏感行为；

d) 预置应用软件的敏感行为明示应对应到具体的行为内容，而不是信息类型。如“读取短信”，而不是“短信”；

e) 通过操作系统弹窗方式申请涉及用户个人信息的“权限”时，不应存在频繁、强制、过度索取“权限”的行为，应参照T/TAF 078.4-2021中的规定。

10.2 个人信息保护

标准要求：预置应用软件不应存在未明确告知用户收集使用个人信息的目的、方式和范围，读取并传送用户个人信息的行为。

测试细则：

预置应用软件应明示个人信息处理规则，明示个人信息处理的目的、方式和范围，并征得用户同意。仅读取个人信息的，应遵照执行。

注1：个人信息包含但不限于10.3中用户数据范围。

注2：法律法规另有规定的除外。

10.3 收集用户数据

标准要求：预置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，包括在用户无确认情况下开启通话录音、本地录音、后台截屏/录屏、拍照/摄像、定位和接收短信，读取用户本机号码、电话本数据、通话记录、短信数据、上网记录、日程表数据、定位信息、读取媒体影音数据（如照片、视频和音频），采集和读取生物特征识别信息（如指纹识别、人脸识别等）、读取设备唯一可识别信息（如不可重置的设备标识符）、应用软件列表的行为。

测试细则：

a) 收集上述用户数据时，不应存在用户拒绝相关行为而退出或关闭，用户数据是应用所必需的除外；

b) 处理定位信息和生物特征识别信息应单独明示并经用户同意；

c) 后台截屏/录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；

d) 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；

e) 预置应用读取短信验证码时，需要明确告知用户场景；

f) 上网记录数据包括浏览记录及书签，原则上不包含用户主动点击加载新网页的行为；

g) 读取设备唯一可识别信息（如不可重置的设备标识符）主要指IMEI和设备MAC地址。

10.4 数据录入保护

标准要求：支付类预置应用软件输入认证/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以明文显示。

测试细则：支付类预置应用，指预置应用自身包含支付模块且可以独立完成支付功能。

10.5 数据加密传输

标准要求：预置应用软件通过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，传感采集类和设备信息类信息；

b) 预置应用软件应采用密文方式传输用户个人摄录的媒体影音类信息。

测试细则：

a) 仅针对通过公共网络传输情况；

b) 敏感数据包括但不限于用户名、口令、账户信息、传感器信息等；

c) 运营商或标准协议要求的不加密场景，如MMS协议要求或运营商要求的RCS消息，可不采用加密方式，需厂家做特殊性声明；

d) 针对个人信息的传输，原则上不应允许传输接收方不支持加密导致明文传输，如特殊情况需对场景进行特别声明。

10.6 应用软件签名

标准要求：

a) 预置应用软件应包含签名信息，且签名信息真实有效。

b) 如果移动智能终端采用认证签名机制，在此情况下，预置应用软件应使用第三方数字证书对其进行签名。

测试细则：

a) 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；

b) 对于非谷歌官方应用，不得采用安卓公开证书；

c) Android/emailAddress=android@android.com，也不能明显与该产品无关的签名如Android Debug等；

d) “应用开发者，公司和部门每一项需保证真实有效，不能为网址、乱码等无效信息，签名证书DN主题项中宜正确标识开发者身份主体信息，如企业名称、组织、省市和国家等信息，不得含有跟主体无关的信息；

e) b）项仅针对采用认证签名机制的终端。

10.7 升级更新要求

标准要求：

a) 预置应用软件或插件更新应在用户授权的情况下进行，不应直接更新；

b) 预置应用软件提供自动更新功能时，应提供自动更新开关，且自动更新功能应默认关闭；

c) 预置应用软件应提供更新包下载可控机制。如无相关机制，则应具备未安装的应用更新包的删除能力；

d) 预置应用软件用户数据库等热更新（应用或插件部分内容更新，无需重启应用软件或资源包）应提示用户并在用户同意后进行更新；

e) 当预置应用软件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，应提示用户可能带来的安全风险；

f) 当预置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：

a,c)预置应用软件升级包含更新包下载和执行更新安装两个行为，两个行为可同时受控或者分开受控均符合要求，但要明确告知用户此行为包含下载和执行。

10.8 调用终端通信功能

10.8.1 流量耗费

标准要求：预置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：

a) 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；

b) 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、短视频和小游戏可作为应用联网行为的明示，在用户点击应用后，发生联网行为，可视为满足标准要求；

c) 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；

d) 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；

e) 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如果是可安装的系统组件可以在桌面入口明示。若只有Widget，如果是可安装的系统组件需满足需要独立明示，需满足YD/T 2407-2021《移动智能终端安全能力技术要求》5.3.5.2操作系统敏感行为安全要求；

f) 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。

10.8.2 费用损失

标准要求：预置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、开启移动通信网络或WLAN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。

10.8.3 信息泄露

标准要求：预置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，包括在用户无确认情况下读取并传送用户本机号码、电话本数据、通话记录、短信数据、上网记录、日程表数据、定位信息、图片、音频、视频等用户个人信息的行为。

测试细则：

a） 上网记录数据包括浏览记录及书签，原则上不包含用户主动点击加载新网页的行为；

b） 定位信息为用户记录位置的相关信息。

10.9 应用软件漏洞要求

标准要求：应保证不含有预置应用软件版本发布日期6个月前CNVD与CNNVD公布的高危及以上漏洞。

测试细则：

a） 测试漏洞采用抽测方式，测试样本按时间递增；

b） 厂商可以进行自证。

10.10 测试模式

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。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：

a） 移动智能终端进行测试时应具备测试模式；

b） 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；

c） 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；

d） 对终端内全部应用的敏感行为的调用日志信息进行显示，仅显示敏感行为调用日志，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。如厂家无法提供仅显示测试相关日志的LOG信息，需提供日志筛选关键字，筛选关键字为“cnalifs”；

e） 日志格式如下，关键字和可安装的系统组件及预置应用软件一一对应，同一类型操作系统应统一。如果进程名可唯一识别可安装的系统组件及预置应用软件，关键字和进程名可相同。

格式：“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

可安装的系统组件敏感行为列表见表2。

表 2 可安装的系统组件敏感行为列表

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/录屏	是	—
4	拍照/摄像（打开摄像头）	是	—
5	接收短信	是	—
6	定位	是	如果接口不同需区分定位类型，如 WLAN，小区基

序号	测试条目（操作）	类型	解读
			站或 GNSS

表 2　可安装的系统组件敏感行为列表（续）

序号	测试条目（操作）	类型	解读
7	采集生物特征识别信息	是	提供生物特征类型，如指纹识别，人脸识别
8	传送生物特征识别信息	可选	提供生物特征类型，如指纹识别，人脸识别
9	读取用户本机号码	是	—
10	读取电话本数据	是	—
11	读取通话记录	是	—
12	读取短信数据	是	—
13	读取彩信数据	是	—
14	读取上网记录	是	—
15	读取日程表数据	是	—
16	传送用户本机号码	可选	保留操作系统差异性
17	传送电话本数据	可选	保留操作系统差异性
18	传送通话记录	可选	保留操作系统差异性
19	传送短信数据	可选	保留操作系统差异性
20	传送上网记录	可选	保留操作系统差异性
21	传送日程表数据	可选	保留操作系统差异性
22	读取图片	是	—
23	读取视频	是	—
24	读取音频	是	—
25	读取生物特征识别信息	是	提供生物特征类型，如指纹识别，人脸识别
26	读取设备唯一可识别信息（IMEI 和设备 MAC 地址）	是	提供信息类型，如 IMEI，MAC
27	读取应用软件列表	是	—
28	拨打电话	是	提供呼叫电话号码
29	发送短信	是	提供接收电话号码
30	发送彩信	是	提供接收电话号码
31	移动通信网络数据连接传送数据	是	提供 IP 信息
32	WLAN 网络连接传送数据	是	提供 IP 信息
33	无线外围接口传送数据	是	提供外围接口类型
34	开启移动通信网络连接	是	开启移动数据开关
35	开启 WLAN	是	开启 WLAN 开关
36	开启无线外围接口	是	提供外围接口类型

移动智能终端预置应用软件敏感行为列表见表3。

表 3　移动智能终端预置应用软件敏感行为列表

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	—

表 3　移动智能终端预置应用软件敏感行为列表（续）

序号	测试条目（操作）	类型	解读
3	后台截屏/录屏	是	如果接口不同需区分
4	拍照/摄像（打开摄像头）	是	如果接口不同需区分
5	接收短信	是	—
6	定位	是	如果接口不同需区分定位类型，如 WLAN，小区基站或 GNSS
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	读取上网记录	是	—
12	读取日程表数据	是	—
13	读取定位信息	是	—
14	读取图片	是	—
15	读取视频	是	—
16	读取音频	是	—
17	采集生物特征识别信息	是	提供生物特征类型，如指纹识别，人脸识别
18	读取生物特征识别信息	是	提供生物特征类型，如指纹识别，人脸识别
19	读取设备唯一可识别信息（IMEI 和设备 MAC 地址）	是	提供信息类型，如 IMEI，MAC
20	读取应用软件列表	是	—
21	删除电话本数据	是	—
22	删除通话记录	是	—
23	删除短信数据	是	—
24	删除日程表数据	是	—
25	修改用户电话本数据	是	—
26	修改通话记录	是	—
27	修改短信数据	是	—
28	修改日程表数据	是	—
29	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
30	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）	可选	保留操作系统差异性
31	网络传输数据信息内容（媒体影音类）	可选	保留操作系统差异性
32	组件暴露测试	可选	测试方法保留操作系统差异性
33	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，如果采用认证签名需提供足够证明

表 3　移动智能终端预置应用软件敏感行为列表（续）

序号	测试条目（操作）	类型	解读
34	应用软件/插件更新	可选	需厂家配合提供测试条件
35	应用软件更新包下载	可选	需厂家配合提供测试条件
36	应用软件热更新	可选	需厂家配合提供测试条件
37	移动通信网络数据连接传送数据	是	提供 IP 信息
38	WLAN 网络连接传送数据	是	提供 IP 信息
39	无线外围接口传送数据	是	—
40	拨打电话	是	提供呼叫电话号码
41	发送短信	是	提供接收电话号码
42	发送彩信	是	提供接收电话号码
43	开启移动通信网络连接	是	开启移动数据开关
44	开启 WLAN	是	开启 WLAN 开关
46	读取并传送用户本机号码	可选	保留操作系统差异性
47	读取并传送电话本数据	可选	保留操作系统差异性
48	读取并传送通话记录	可选	保留操作系统差异性
49	读取并传送短信数据	可选	保留操作系统差异性
50	读取并传送上网记录	可选	保留操作系统差异性
51	读取并传送日程表数据	可选	保留操作系统差异性
52	读取并传送定位信息	可选	保留操作系统差异性
53	读取并传送图片	可选	保留操作系统差异性
54	读取并传送音频	可选	保留操作系统差异性
55	读取并传送视频	可选	保留操作系统差异性

参 考 文 献

[1] T/TAF 078.4-2021 APP 用户权益保护测评规范 第 4 部分：权限索取行为

电信终端产业协会团体标准

移动智能终端安全能力测试细则

T/TAF 047—2022

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn