电信终端产业协会标准

TAF-WG4-AS0015-V1.0.0:2018

移动智能终端安全能力技术要求

Technical requirements for security capability of smart mobile terminal

2018 - 03- 01 发布　　2018 - 03- 01 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、中国移动通信集团公司、中国联合网络通信集团有限公司、浙江蚂蚁小微金融服务集团有限公司、深圳酷派技术有限公司。

本标准主要起草人： 姚一楠、潘娟、杨正军、国炜、傅山、翟世俊、焦四辈、王宗岳、孙龙、汪薇薇、詹维骁、谢春霞、袁杰、邱勤、周晶、落红卫、叶瑞权。

引　　言

随着移动智能终端的广泛应用以及功能的不断扩展，其使用过程中的安全问题被越来越多的用户所关注。近年来，恶意吸费、窃听、窃录、位置信息泄露等安全事件频发，使用户对移动智能终端的安全性产生顾虑，进而影响到移动智能终端和移动互联网应用的发展。本标准的制定，旨在通过提高移动智能终端的自身的安全防护能力，防范移动智能终端上的各种安全威胁，避免用户的利益受到损害，同时防止移动智能终端对移动通信网络安全产生不利影响。

本标准的基本原则是：移动智能终端上发生的行为和应用要符合用户的意愿。本标准并不规定具体的实现方法和措施，以利于创新和发展。本标准从硬件安全能力要求、操作系统安全能力要求、外围接口安全能力要求、应用软件安全要求、用户数据安全保护能力要求5个层面对移动智能终端的安全能力提出了要求，并从基本的安全保障、实现难度、特殊安全能力等层面对安全能力进行了分级，以便于产品具有特定品质，便于消费者选择。通过本标准一方面能够引导移动智能终端中预置应用软件更加规范、安全；另一方面也能引导移动智能终端提高自身的安全防护能力，可对后下载的第三方应用进行安全管控；同时也能防范移动智能终端中预置恶意代码对网络造成安全影响。

移动智能终端安全能力技术要求

1 范围

本标准规定了移动智能终端安全能力的技术要求，包括移动智能终端的硬件安全能力、操作系统安全能力、外围接口安全能力、应用层安全要求和用户数据保护安全能力等，并对安全能力进行了分级。

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。

2 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 1699-2007　移动终端信息安全技术要求

YD/T 1760-2012　数字移动终端外围接口数据交换技术要求

YD/T 3228-2017　移动应用软件安全评估方法

YD/T 3082-2016　移动智能终端上的个人信息保护技术要求

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

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。

3.1.2

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。

3.1.3

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。

3.1.4

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。

3.1.5

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。

3.1.6

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。

3.1.7

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。

3.1.8

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接口。

3.1.9

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。

3.2　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

4　移动智能终端安全能力框架及目标

4.1　移动智能终端安全能力框架

移动智能终端安全能力主要由硬件安全能力、操作系统安全能力、应用层安全要求、外围接口安全能力和用户数据保护安全能力五部分构成，具体如图1所示。

外围接口安全能力涉及操作系统和硬件，用户数据保护安全能力涉及硬件、操作系统和应用软件3个层面。

<table>
<tr><td colspan="2">应用层安全要求</td><td rowspan="3">用户数据保护安全能力</td></tr>
<tr><td>操作系统安全能力</td><td rowspan="2">外围接口安全能力</td></tr>
<tr><td>硬件安全能力</td></tr>
</table>

图1 移动智能终端安全能力框架

4.2　移动智能终端安全目标

4.2.1 硬件安全目标

移动智能终端硬件安全目标是在芯片层保证移动通信终端内部闪存和基带的安全，确保芯片内系统程序、终端参数、安全数据、用户数据不被篡改或非法获取。

4.2.2 操作系统安全目标

操作系统安全目标是达到操作系统对系统资源调用的监控、保护和提醒，确保涉及安全的系统行为总是在受控的状态下，不会出现用户在不知情情况下某种行为的执行，或者用户不可控行为的执行。另外，操作系统还应保证自身的升级是受控的。

4.2.3 外围接口安全目标

外围接口包括无线外围接口和有线外围接口。外围接口的安全目标是确保用户对外围接口的连接及数据传输的可知和可控。

4.2.4 应用层安全目标

应用层安全目标是要保证移动智能终端对要安装在其上的应用软件可进行来源的识别，对已经安装在其上的应用软件可以进行敏感行为的控制。另外，还要确保预置在移动智能终端中的应用软件无损害用户利益和危害网络安全的行为，例如恶意吸费、未经授权的修改、删除、向外传送用户数据等行为。

4.2.5 用户数据保护安全目标

用户数据保护安全目标是要保证用户数据的安全存储，确保用户数据不被非法访问、获取和篡改，同时能够通过备份方式保证用户数据的可靠恢复。

5 移动智能终端安全能力技术要求

5.1 基本要求

移动智能终端应通过给用户提示和让用户确认的方式来防范安全威胁，当第三方应用调用相关功能时，操作系统应具备给用户提示和让用户确认的能力；预置多操作系统的移动智能终端，每一个操作系统在运行过程中都应具备给用户提示和让用户确认的能力。

给用户的提示可以是图标、文字或其他明显的提示方式。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。

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。

用户确认如无特别说明，则认为以下三种确认方式均可：

— 应用软件每一次调用行为发生时进行确认；

— 应用软件首次调用行为发生时确认，本确认在一定时间内有效，确认应针对每一个调用行为单独确认；

— 应用软件首次安装或调用行为发生时确认，本确认对该软件长期有效，确认应针对每一个调用行为单独确认。

本章所提及的给用户提示和用户确认，均指由第三方应用调用相关功能时，操作系统所应具备的能力。对于第三方应用通过调用操作系统提供的人—机接口执行的操作，认为是在用户知情的情况下执行的操作，已经给用户提示并得到用户的确认。

对于应用软件安全配置中用户设置为允许访问的操作，也认为是在用户知情的情况下执行的操作，已经得到用户的确认。

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在任何情况下都应给用户提示并经用户确认。

5.3 和 5.4 节所提及的安全能力要求，仅适用于当第三方应用调用操作系统提供的相应功能的情况。5.5.1、5.5.2、5.5.3 和 5.5.4 所提及的应用软件是指非预置的应用软件。

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。

移动智能终端操作系统不应有未向用户明示且未经用户同意，擅自调用终端功能，造成用户费用损失，流量耗费，信息泄漏的行为。

5.2 移动智能终端硬件安全能力要求

5.2.1 安全运行区域

移动智能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。

5.2.2 安全启动

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。

5.2.3 防止物理攻击

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。

5.2.4 安全属性

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。

5.2.5 根密钥生成与保护

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。

5.3 移动智能终端操作系统安全能力要求

5.3.1 安全调用控制能力

5.3.1.1 通信类功能受控机制

5.3.1.1.1 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。

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。

5.3.1.1.2 三方通话

应用软件调用执行三方通话操作时，应在用户确认的情况下，三方通话操作才能执行。

5.3.1.1.3 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。

5.3.1.1.4 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。

5.3.1.1.5 发送邮件

应用软件调用执行发送邮件操作时，应在用户确认的情况下，邮件发送操作才能执行。

5.3.1.1.6 移动通信网络数据连接

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：

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；

b）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；

c）移动通信网络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；

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；

e）当移动通信网络正在传送数据时，移动智能终端应在用户主界面上给用户相应的状态提示。

上述c）和e）的两种状态提示应不同。

5.3.1.1.7 WLAN 网络连接

移动智能终端WLAN网络连接应满足以下安全能力要求：

a）移动智能终端应提供开关，可开启/关闭WLAN网络连接；

b）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；

c）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；

d）当WLAN网络正在传送数据时，移动智能终端应在用户主界面上给用户相应的状态提示。

上述c）和d）的两种状态提示应不同。

5.3.1.2 本地敏感功能受控机制

5.3.1.2.1 定位功能

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。调用后，移动智能终端应在用户主界面上给用户相应的状态提示。

5.3.1.2.2 通话录音功能

通话录音是指在通话状态下录取线路上双方的话音。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。

5.3.1.2.3 本地录音功能

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。

5.3.1.2.4 后台截屏功能

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。

5.3.1.2.5 拍照/摄像功能

对于具备摄像头的移动智能终端，当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（图像预览、指示灯、声音或图标等），在用户确认的情况下方可执行拍照或摄像操作。

5.3.1.2.6 接收短信功能

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。

5.3.1.2.7 对用户数据的操作

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。

5.3.2 操作系统的更新

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；

5.3.3 操作系统隔离要求

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。

5.3.4 操作系统漏洞要求

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。

5.4 移动智能终端外围接口安全能力要求

5.4.1 无线外围接口安全能力要求

5.4.1.1 无线外围接口开启/关闭受控机制

对于具备蓝牙、NFC功能的移动智能终端应具备开关，可开启/关闭蓝牙、NFC等终端所支持的无线连接方式。

当应用软件调用开启无线外围接口时，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。

5.4.1.2 无线外围接口连接建立的确认机制

当通过无线外围接口（仅适用于蓝牙）与不同设备进行第一次连接时，移动智能终端能够发现该连接并给用户相应的提示，当用户确认建立连接时，连接才可建立。

示例：蓝牙配对机制。

5.4.1.3 无线外围接口连接状态提示

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。

5.4.1.4 无线外围接口数据传输的受控机制

当移动智能终端与其他设备已经通过无线外围接口（蓝牙或NFC）实现连接，此时通过无线外围接口进行文件数据传输时，移动智能终端应给用户相应的提示。

5.4.2 有线外围接口安全能力要求

5.4.2.1 有线外围接口连接建立的确认机制

对于仅用于充电或仅用于数据连接的有线外围接口，当通过该接口建立连接时，移动智能终端应给用户相应的提示。

对于既可进行充电，又可进行数据连接的有线外围接口，当连接充电器时应给用户相应的提示，当连接于既可进行充电又可进行数据连接的设备时，用户应能够选择是否建立数据连接模式或者能够保证数据传输授权可控。

5.4.2.2 USB 存储模式的安全机制

如果移动智能终端支持内置式USB存储模式（U盘模式），则应提供访问控制方式。

5.5 移动智能终端应用层安全要求

5.5.1 应用软件安全配置能力要求

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。

5.5.2 应用软件调用行为记录能力要求

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。

5.5.3 应用软件安全认证机制要求

5.5.3.1 非认证签名要求

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。

5.5.3.2 认证签名要求

如果移动智能终端采用认证签名机制，在此情况下，未经过认证签名的应用软件仅当用户进行确认后才能执行下一步操作。

5.5.4 应用软件自启动监控能力

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。

5.5.5 预置应用软件安全要求

5.5.5.1 收集用户数据

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、拍照/摄像、接收短信和定位，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、定位信息的行为。

b）在用户无确认情况下读取图片、音频和视频的行为。

5.5.5.2 修改用户数据

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、日程表数据的行为。

5.5.5.3 数据录入保护

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。

5.5.5.4 数据加密传输

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；

b）预置应用软件应采用密文方式传输媒体影音类信息。

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》。

5.5.5.5 组件访问控制

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。

5.5.5.6 软件认证签名

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。

5.5.5.7 升级更新要求

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。

5.5.5.8 调用终端通信功能

5.5.5.8.1 流量耗费

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。

5.5.5.8.2 费用损失

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。

5.5.5.8.3 信息泄露

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、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。

5.5.5.9 应用软件漏洞要求

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。

5.6 移动智能终端用户数据安全保护能力要求

5.6.1 移动智能终端的密码保护

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）。

5.6.2 文件类用户数据的授权访问

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。

5.6.3 用户数据的加密存储

未经授权的任何实体应不能从移动智能终端的加密存储区域的数据中还原出用户私密数据的真实内容。

5.6.4 用户数据的彻底删除

移动智能终端提供数据彻底删除功能，以保证被删除的用户数据不可再恢复出来。一般的删除功能仅会删除数据在存储器件中放置位置的索引，而该区域内实际存储的数据没有完全清空，在数据被删除之后，非法程序通过读取该区域的内容，仍有可能从读取到的数据中恢复被删除的私密数据。彻底删除功能应把该区域内实际存储的数据彻底消除。例如，当终端用户数据被删除时，在该数据对应的存储区域使用全“0”或全“1”进行多次填充。

5.6.5 用户数据的远程保护

移动智能终端应提供用户数据的远程保护能力，以便用户在手机遗失或其他情况下，终端中的用户数据不被泄露。远程保护能力包括远程锁定移动智能终端和远程销毁用户数据。移动智能终端提供的远程保护功能也应具备安全设置，确保远程保护功能仅在达到了用户预设条件的情况下才会启动。

该功能可参考开放移动联盟（OMA）组织发布的标准OMA-TS-LAWMO《锁定和彻底删除管理对象》。

5.6.6 用户数据的转移备份

移动智能终端应具备用户数据（至少包括电话本、短信、多媒体数据）的转移及备份能力。

用户数据的转移备份包括本地备份和远程备份两种：本地备份是通过移动智能终端的外围接口实现的数据备份；远程备份是通过无线网络实现的用户数据在服务器侧的备份。本地备份适用于支持外围接口的移动智能终端。移动智能终端应至少支持一种备份方式。

用户数据的转移和备份应符合YD/T 1760-2012的相关要求。

6 移动智能终端功能限制性要求

移动智能终端应真实传送信息，不得通过对传送信息的处理或传送虚假信息使信息接收者错误识别特定通信主体等，不得预置可改变通信系统提示信号的应用软件。

移动智能终端不得预置国家法律法规禁止的信息内容（包括但不限于预置图片、文字、菜单、音视频、应用等），也不得预置为传播发布国家法律法规禁止信息内容提供服务的应用软件。

7 移动智能终端安全能力分级

7.1 概述

移动智能终端所支持的安全能力划分为五个等级，第五级是最高等级。移动智能终端可选支持到不同的等级。达到相应等级的移动智能终端可在说明书上进行明确的标识，预置多操作系统的移动智能终端，每一操作系统所支持的安全能力等级可分别进行标识，参见附录A的内容。

7.2 安全能力分级

根据移动智能终端所支持的安全能力的程度，将移动智能终端安全能力自低到高划分为五个等级。在每一等级定义了移动智能终端在相应等级对应的安全能力的最小集合，也就是移动智能终端必须支持该集合中的所有安全能力才能标识为该级别，例如：达到第五级的移动智能终端应支持本标准第5章和第6章所定义的所有安全能力及功能限制性要求。具体的等级划分详见表1。

表 1 移动智能终端安全能力分级

安全能力		安全能力等级				
		一级	二级	三级	四级	五级
1.	5.2.1 安全运行区域					√
2.	5.2.2 安全启动					√
3.	5.2.3 防止物理攻击					√
4.	5.2.4 安全属性					√
5.	5.2.5 根密钥生成与保护					√
6.	5.3.1.1.1 拨打电话	√	√	√	√	√
7.	5.3.1.1.2 三方通话		√	√	√	√
8.	5.3.1.1.3 发送短信	√	√	√	√	√
9.	5.3.1.1.4 发送彩信					√
10.	5.3.1.1.5 发送邮件					√
11.	5.3.1.1.6a）移动通信网络数据连接—开关	√	√	√	√	√
12.	5.3.1.1.6b）移动通信网络数据连接—应用调用时的确认	√	√	√	√	√
13.	5.3.1.1.6c）移动通信网络数据连接—连接状态提示	√	√	√	√	√
14.	5.3.1.1.6d）移动通信网络数据连接—数据传送时的确认	√	√	√	√	√
15.	5.3.1.1.6e）移动通信网络数据连接—数据传送状态提示		√	√	√	√
16.	5.3.1.1.7a）WLAN 网络连接—开关	√	√	√	√	√
17.	5.3.1.1.7b）WLAN 网络连接—应用调用时的确认	√	√	√	√	√
18.	5.3.1.1.7c）WLAN 网络连接—连接状态提示	√	√	√	√	√
19.	5.3.1.1.7d）WLAN 网络连接—数据传送状态提示			√	√	√
20.	5.3.1.2.1 定位功能	√	√	√	√	√
21.	5.3.1.2.2 通话录音功能	√	√	√	√	√
22.	5.3.1.2.3 本地录音功能	√	√	√	√	√
23.	5.3.1.2.4 后台截屏功能	√	√	√	√	√
24.	5.3.1.2.5 拍照/摄像功能	√	√	√	√	√
25.	5.3.1.2.6 接收短信功能	√	√	√	√	√
26.	5.3.1.2.7a）对用户数据的操作—修改/删除				√	√
27.	5.3.1.2.7b）对用户数据的操作—读	√	√	√	√	√
28.	5.3.2a）操作系统的更新—授权更新			√	√	√
29.	5.3.2b）操作系统的更新—风险提示	√	√	√	√	√

30.	5.3.3 操作系统隔离要求				√	√
31.	5.3.4 操作系统漏洞要求					√
32.	5.4.1.1 无线外围接口开启/关闭受控机制	√	√	√	√	√
33.	5.4.1.2 无线外围接口连接建立的确认机制	√	√	√	√	√
34.	5.4.1.3 无线外围接口连接状态标识	√	√	√	√	√
35.	5.4.1.4 无线外围接口数据传输的受控机制				√	√
36.	5.4.2.1 有线外围接口连接建立的确认机制			√	√	√
37.	5.4.2.2 U 盘模式的安全机制			√	√	√
38.	5.5.1 应用软件安全配置能力要求				√	√
39.	5.5.2 应用软件调用行为记录能力要求					√
40.	5.5.3.1 非认证签名要求	√	√	√	√	√
41.	5.5.3.2 认证签名要求			√	√	√
42.	5.5.4 应用软件自启动程序监控能力			√	√	√
43.	5.5.5.1a）收集用户数据—敏感数据	√	√	√	√	√
44.	5.5.5.1b）收集用户数据—多媒体数据				√	√
45.	5.5.5.2 修改用户数据	√	√	√	√	√
46.	5.5.5.3 数据录入保护				√	√
47.	5.5.5.4a）数据加密传输—敏感数据			√	√	√
48.	5.5.5.4b）数据加密传输—多媒体数据					√
49.	5.5.5.5 组件访问控制			√	√	√
50.	5.5.5.6 软件认证签名	√	√	√	√	√
51.	5.5.5.7 升级更新要求			√	√	√
52.	5.5.5.8.1 流量耗费	√	√	√	√	√
53.	5.5.5.8.2 费用损失	√	√	√	√	√
54.	5.5.5.8.3a）信息泄露—敏感数据	√	√	√	√	√
55.	5.5.5.8.3b）信息泄露—多媒体数据				√	√
56.	5.5.5.9 应用软件漏洞要求					√
57.	5.6.1a）移动智能终端的密码保护—开机及密码保护	√	√	√	√	√
58.	5.6.1b）移动智能终端的密码保护—锁定状态数据保护				√	√
59.	5.6.2 文件类用户数据的授权访问					√
60.	5.6.3 用户数据的加密存储					√
61.	5.6.4 用户数据的彻底删除			√	√	√
62.	5.6.5 用户数据的远程保护		√	√	√	√
63.	5.6.6 用户数据的转移备份		√	√	√	√
64.	6 移动智能终端功能限制性要求	√	√	√	√	√

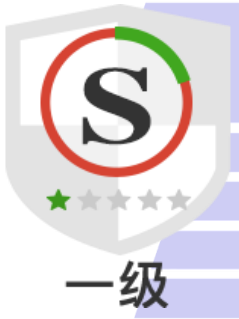
附　录　A
（资料性附录）
安全能力等级标识

本附录给出了移动智能终端在说明书/包装盒上进行相应等级标注的形式，推荐终端厂商按照本附录的要求给用户提供相应的标注。

标注分为两个部分：

— 移动智能终端安全能力等级标识：该标识标明了移动智能终端所达到的安全能力级别，按照安全能力分级要求分为5个等级。标识的图案如图A.1所示。

— 移动智能终端安全功能丰富度标识：在对移动智能终端安全能力等级进行标识后，可进一步对移动智能终端安全功能丰富度进行标识。该标识标明了移动智能终端具备的安全相关功能的个数，安全相关功能包括WLAN、定位、拍照/摄像、蓝牙和NFC。标识的图案如图A.2所示。

				
一级	二级	三级	四级	五级

注：图中绿色部分的个数代表所达到的级别，绿色越多代表越安全，最高级别为五级。

图A.1　移动智能终端安全能力等级标识

				
支持一种功能	支持两种功能	支持三种功能	支持四种功能	支持五种功能

注：以达到三级安全级别的标识为例，图中圆圈内黄色线条的个数代表了移动智能终端所支持的安全相关功能的个数，黄色线条越多代表支持的安全功能越多，最多支持五种安全功能。

图A.2　移动智能终端安全功能丰富度标识

参 考 文 献

[1] Q/CUP 037.1.2-2011 中国银联移动支付技术规范第1卷：基础规范 第2部分 移动终端支付应用用软件安全规范

[2] OMA-TS-LAWMO 锁定和删除管理对象