ICS 33.050
CCS M 30

团　体　标　准

T/TAF 172—2023

循环回收移动智能通信终端信息安全技术要求和测试方法

Test methods for security capability of the recyclable mobile communication terminal

2023-07-20 发布　　2023-07-20 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。

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：深圳信息通信研究院、中国信息通信研究院、中信数字媒体网络有限公司、北京转转精神科技有限责任公司、深圳闪回科技有限公司、华为技术有限公司、OPPO广东移动通信有限公司。

本文件主要起草人：肖雳、张博钧、唐伟生、苏章凯、李鹏、王佳、史伟进、孟祥东、高媛媛、张旭、刘晨、邱强、黄曼琪、黄炜、马求斌、闫杰、刘剑逸、彭志勇、赵砚博、张悦、劳君杰。

引　言

目前我国二手手机市场错综复杂，对于消费者，也存在交易前后用户一些高度涉及用户隐私的软硬件被非法使用或者被植入监控模块，威胁用户的隐私与通信安全。这严重影响了用户对二手市场的可信度并制约着二手移动智能通信终端市场的发展。

为坚决贯彻我国“十四五”循环经济发展规划，促进我国循环经济的发展，保障国家资源安全，推动实现碳达峰、碳中和，促进生态文明建设，现迫切需要制定二手移动智能通信终端信息安全技术要求和测试方法，切实保障二手移动智能通信终端在整个交易链条中的信息安全，保障广大消费者利益。

本文件主要针对循环回收移动智能通信终端产品信息安全相关的用户数据保护安全能力、预置第三方应用安全能力、操作系统安全能力等方面展开研究，并研究制定相关的测试方法。

循环回收移动智能通信终端信息安全技术要求和测试方法

1 范围

本文件规定了循环回收移动智能通信终端安全能力的技术要求和测试方法，包括用户数据保护安全能力、预置第三方应用安全能力、操作系统安全能力。

本文件适用于各种制式的循环回收移动智能通信终端。

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

3 术语和定义

下列术语和定义适用于本文件。

3.1

移动智能通信终端 smart mobile terminal

能够接入公用电信网，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移动通信终端。

3.2

循环回收移动智能通信终端 recyclable mobile communication terminal

首次销售后再次进入市场流通的、不涉及非法和侵权的移动智能通信终端。

3.3

安全能力 security capability

在移动智能通信终端上可实现的，能够防范安全威胁的技术手段。

3.4

用户 user

使用移动智能通信终端资源的对象，包括人或第三方应用软件。

3.5

用户数据 user data

移动智能通信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。

3.6

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。

3.7

预置第三方应用软件　preinstalled applications

移动智能通信终端内，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非系统原生或本机终端厂商自研的应用软件。

4　安全能力框架及目标

4.1 安全能力框架

循环回收移动智能通信终端安全能力主要由操作系统安全能力、用户数据保护安全能力和预置第三方应用安全能力构成。

4.2 安全目标

4.2.1　操作系统安全目标

操作系统包含常规智能操作系统自身及操作系统组件和服务，以及镶嵌在智能操作系统中提供相应开放接口供应用软件（框架应用软件，如免安装应用等）使用的框架。

操作系统安全目标是操作系统无损害用户利益和危害网络和终端安全的行为，以及提供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。

4.2.2　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。

5　安全能力技术要求

5.1 基本要求

循环回收移动智能通信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，当操作系统自身或者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。

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。

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。

本文 5.4 节所提及的给用户提示和用户确认，均指由系统自身或者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一机接口执行的操作，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。

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 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。

循环回收移动智能通信终端预置第三方应用软件需满足无损害用户利益和危害网络或终端安全的行为。

5.2 用户数据安全保护能力要求

5.2.1 密码保护

循环回收移动智能通信终端密码保护功能，应满足以下安全能力要求：

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。

5.2.2 用户数据的彻底删除

循环回收移动智能通信终端应保证彻底删除用户数据（包括但不限于通话记录、短信、彩信、通讯录、日程表、影音数据、账号信息等）且应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，非法软件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。彻底删除应把该区域内实际存储的数据彻底删除。

5.3 预置第三方应用安全保护能力要求

5.3.1 收集用户数据

循环回收移动智能通信终端中预置的第三方应用软件不应有未向用户明示并经用户同意，擅自收集用户个人信息的行为，包括在用户无确认的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、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、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。

5.3.2 修改用户数据

循环回收移动智能通信终端中预置的第三方应用软件不应有未向用户明示并经用户同意，擅自修改用户个人信息的行为，包括在用户无确认情况下修改（包含写和删除）用户电话本数据、通话记录、短信数据、日程表数据的行为。

5.3.3 流量耗费

循环回收移动智能通信终端中预置的第三方应用软件不应有未向用户明示并经用户同意，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。

5.3.4 费用损失

循环回收移动智能通信终端中预置的第三方应用软件不应有未向用户明示并经用户同意，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。

5.3.5 信息泄露

循环回收移动智能通信终端中预置的第三方应用软件不应有未向用户明示并经用户同意，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、日程表信息、定位信息、图片、音频、视频等用户个人信息行为。

5.4 操作系统安全能力要求

5.4.1 通信类功能受控机制

5.4.1.1 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。

5.4.1.2 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。

5.4.2 本地敏感功能受控机制

5.4.2.1 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。

5.4.2.2 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。

5.4.2.3 对用户数据的操作

移动智能通信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：

当应用软件需要调用对通话记录、短信数据、通讯录的读操作时，移动智能通信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。

6 安全能力测试方法

6.1 概述及基本要求

本章描述了针对移动智能终端的各种安全能力进行评测的方法。评测结果有以下三种：

——未见异常：通过评测方法没有发现存在安全风险或安全事件；

——不符合要求：直接发现安全事件或不符合安全能力要求；

——不支持：终端不支持相应功能。

6.2 用户数据安全保护能力测试方法

6.2.1 密码保护

测试项目：开机密码保护
项目要求：见第 5.2.1 节
预置条件：被测移动智能通信终端关机，终端开启了用户身份认证功能
测试步骤： 步骤 1：将移动智能通信终端开机，终端提示输入用户登录口令； 步骤 2：输入正确的用户口令； 步骤 3：通过终端的人-机界面，进入用户登录口令更改菜单； 步骤 4：修改用户登录口令为 3 位数； 步骤 5：修改用户登录口令为 4 位数或 4 位以上数字； 步骤 6：关机，再开机； 步骤 7：输入旧密码； 步骤 8：输入新密码； 步骤 9：通过终端的人-机界面，进入用户登录口令菜单，关闭用户身份认证功能； 步骤 10：关机，再开机； 步骤 11：通过终端的人-机界面，将用户登录口令修改为正常值； 步骤 12：关机，再开机； 步骤 13：持续输入错误的用户口令（4 位或 4 位以上数）。
预期结果： 在步骤 2 后，移动智能通信终端提示输入口令正确，终端正常开机； 在步骤 4，终端应提示用户登录口令长度过短，请求用户重新输入或者终端无法修改为 3 位数密码； 在步骤 5，用户登录口令修改成功； 在步骤 7，终端应提示登录口令错误；

在步骤 8 后，终端应提示输入口令正确，终端正常开机； 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登录口令，输入正常，终端应提示用户身份认证功能成功关闭； 在步骤 10 后，终端开机过程应不提示用户输入用户登录口令，终端正常开机； 在步骤 13，多次输入错误的用户登录口令后（根据厂商声称，不多于 10 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和锁死等。 循环回收移动智能通信终端满足以上预期结果，则该项目评测结果为“未见异常”，反之该项目评测结果为“不符合要求”。

测试项目：开机后锁定状态的密码保护
项目要求：见第 5.2.1 节
预置条件：被测移动智能通信终端关机，终端开启了用户身份认证功能
测试步骤： 步骤 1：将终端开机，进入屏保菜单，启动屏保激活身份认证； 步骤 2：保持终端处于空闲状态； 步骤 3：使用另一终端拨打被测终端，被测终端按接听键； 步骤 4：呼叫结束； 步骤 5：通过手机键盘激活系统； 步骤 6：输入错误的口令； 步骤 7：输入正确的口令； 步骤 8：通过菜单关闭屏保激活身份认证； 步骤 9：输入正确的口令；
预期结果： 在步骤 1，终端应提示输入屏保激活身份认证的口令； 在步骤 2，在超过等待时间后，终端应进入屏保状态； 在步骤 3，终端应可以正常接听电话； 在步骤 4，呼叫结束后，终端应立即进入屏保状态； 在步骤 5，终端应提示用户输入屏保激活身份认证口令； 在步骤 6，终端应提示口令错误； 在步骤 7：终端应提示口令正确，移动智能通信终端被激活，进入正常使用状态； 在步骤 8，终端应提示输入口令； 在步骤 9，终端应提示屏保激活身份认证被成功关闭。 循环回收移动智能通信终端满足以上预期结果，则该项目评测结果为“未见异常”，反之该项目评测结果为“不符合要求”。

6.2.2 用户数据的彻底删除

测试项目：用户数据的彻底删除
项目要求：见第 5.2.2 节
预置条件：被测移动智能通信终端处于正常工作状态
测试步骤： 步骤 1：检查移动智能通信终端是否可以直接查看用户数据（包括通话记录、短信、彩信、通讯录、日程表、图片、视频、音频、系统账号信息、应用软件登录账号信息等）； 步骤 2：使用应用程序访问终端用户数据（包括通话记录、短信、彩信、通讯录、日程表、图片、视频、音频、系统账号信息、应用软件登录账号信息） 步骤 3：使用数据恢复工具，对终端进行用户数据（包括通话记录、短信、彩信、通讯录、日程表、图片、视频、音频、系统账号信息、应用软件登录账号信息）恢复，查看是否可恢复用户数据信息。
预期结果： 步骤 1 后，如果终端可直接查看用户数据，则该项判断为“不符合要求”，评测结束； 步骤 2 后，如果应用程序可访问到终端用户数据，则该项判断为“不符合要求”，评测结束； 步骤 3 后，如果终端可直接恢复用户数据，则该项判断为“不符合要求”，评测结束；如果终端无法恢复用户数据信息，则该项评测结果为“未见异常”，评测结束。

6.3 预置第三方应用软件安全保护能力测试方法

测试项目：预置第三方应用软件安全保护能力测试方法
项目要求：见第 5.3 节
预置条件：被测移动智能通信终端处于正常工作状态
测试步骤： 步骤 1：使预置应用软件信息安全测试系统（包括服务器和客户端软件）处于正常工作状态； 步骤 2：将预置应用软件信息安全测试系统客户端软件安装到被测移动智能通信终端上，并与服务器建立连接； 步骤 3：使用基于特征码扫描、静态源代码分析和动态行为监测等检测方法，对被测移动智能通信终端预置第三方应用软件未向用户明示并经用户同意，擅自收集用户数据、修改用户数据、流量耗费、费用损失、信息泄露中规定的行为进行检测。
预期结果： 如果预置应用软件信息安全测试系统显示被测移动智能通信终端预置第三方应用软件无擅自收集用户数据、修改用户数据、流量耗费、费用损失、信息泄露中规定的行为，则该项目评测结果为“未见异常”；否则，该项目评测结果为“不符合要求”。

6.4 操作系统安全能力测试方法

6.4.1 通信类功能受控机制

6.4.1.1 拨打电话

测试项目：拨打电话的受控机制
项目要求：见第 5.4.1.1 节
预置条件：被测移动智能通信终端处于正常工作状态
测试步骤： 步骤 1：检查被测移动智能通信终端的操作系统是否提供拨打电话的开发功能； 步骤 2：如果移动智能通信终端操作系统提供拨打电话的开发功能，使用该功能开发拨打电话的应用程序； 步骤 3：运行该应用程序，查看终端是否要求用户确认拨打电话。
预期结果： 在步骤 1 后，如果终端不提供拨打电话的开发功能，则该项的评测结果为“未见异常”； 在步骤 3 后，如果终端要求用户确认拨打电话，则该项评测结果为“未见异常”，评测结束； 在步骤 3 后，如果终端不要求用户确认，并成功拨打电话，则该项评测结果为“不符合要求”，评测结束。

6.4.1.2 发送短信

测试项目：发送短信的受控机制
项目要求：见第 5.4.1.2 节
预置条件：被测移动智能通信终端处于正常工作状态
测试步骤： 步骤 1：检查被测移动智能通信终端的操作系统是否提供发送短信的开发功能； 步骤 2：如果移动智能通信终端操作系统提供发送短信的开发功能，使用该功能开发发送短信的应用程序； 步骤 3：运行该应用程序，查看终端是否要求用户确认发送短信。
预期结果： 在步骤 1 后，如果终端不提供发送短信的开发功能，则该项的评测结果为“未见异常”； 在步骤 3 后，如果终端要求用户确认发送短信，则该项评测结果为“未见异常”，评测结束； 在步骤 3 后，如果终端不要求用户确认，并成功发送短信，则该项评测结果为“不符合要求”，评测结束。

6.4.2 本地敏感功能受控机制

6.4.2.1 通话录音功能

测试项目：通话录音的受控机制
项目要求：见第 5.4.2.1 节
预置条件：被测移动智能通信终端处于正常工作状态

测试步骤： 步骤 1：检查被测移动智能通信终端的操作系统是否提供通话录音的开发功能； 步骤 2：如果移动智能通信终端操作系统提供通话录音的开发功能，使用该功能开发通话录音的应用程序； 步骤 3：运行该应用程序，查看终端是否要求用户确认通话录音；
预期结果： 在步骤 1 后，如果终端不提供通话录音的开发功能，则该项的评测结果为“未见异常”； 在步骤 3 后，如果终端要求用户确认开始通话录音，则该项评测结果为“未见异常”，评测结束； 在步骤 3 后，如果终端不要求用户确认，并成功进行通话录音，则该项评测结果为“不符合要求”，评测结束。

6.4.2.2 本地录音功能

测试项目：本地录音的受控机制
项目要求：见第 5.4.2.2 节
预置条件：被测移动智能通信终端处于正常工作状态
测试步骤： 步骤 1：检查被测移动智能通信终端的操作系统是否提供本地录音的开发功能； 步骤 2：如果移动智能通信终端操作系统提供本地录音的开发功能，使用该功能开发本地录音的应用程序； 步骤 3：运行该应用程序，查看终端是否要求用户确认本地录音；
预期结果： 在步骤 1 后，如果终端不提供本地录音的开发功能，则该项的评测结果为“未见异常”； 在步骤 2 后，如果终端要求用户确认开始本地录音，则该项评测结果为“未见异常”，评测结束； 在步骤 2 后，如果终端不要求用户确认，并成功进行本地录音，则该项评测结果为“不符合要求”，评测结束。

6.4.2.3 对用户数据的操作

测试项目：用户数据的读操作受控机制
项目要求：见第 5.4.2.3 节
预置条件：被测移动智能通信终端处于正常工作状态
测试步骤： 步骤 1：检查被测移动智能通信终端的操作系统是否提供用户数据读取（读取通话记录、读取短信数据、读取通讯录）的开发功能； 步骤 2：如果移动智能通信终端操作系统提供用户数据读取（读取通话记录、读取短信数据、读取通讯录）的开发功能，分别使用该功能开发读取通话记录、读取短信数据、读取通讯录的应用

程序； 步骤 3：分别运行应用程序，检查对应的应用程序安装或首次运行时是否给用户提示；
预期结果： 在步骤 1 后，如果终端不提供用户数据读取（读取通话记录、读取短信数据、读取通讯录）的开发功能，则该项的评测结果为“未见异常”； 在步骤 3 后，如果终端给用户提示应用程序会访问对应的数据（通话记录数据、短信数据、通讯录数据），则该项评测结果为“未见异常”，评测结束； 在步骤 3 后，如果终端没有给用户任何提示，并且应用程序可以成功访问到对应的数据（通话记录数据、短信数据、通讯录数据），则该项评测结果为“不符合要求”，评测结束。

电信终端产业协会团体标准

循环回收移动智能通信终端信息安全技术要求

T/TAF 172—2023

*

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