ICS 33.050
M 30

中华人民共和国国家标准

GB/T 39576—2020

具有融合功能的移动终端安全能力测试方法

Test methods for security capability of mobile terminal with syncretic function

2020-12-14 发布　　2021-07-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由中华人民共和国工业和信息化部提出。

本标准由全国通信标准化技术委员会(SAC/TC 485)归口。

本标准起草单位:中国信息通信研究院、高通无线通信技术(中国)有限公司、真珍斑马技术(上海)贸易有限公司、联想移动通信科技有限公司。

本标准主要起草人:姚一楠、陈婉莹、董霁、翟世俊、王宇晓、王嘉义、杜志敏、翁元、李欣。

引　言

随着移动互联网的快速发展，传统智能终端手机、平板电脑等，并不能完全满足用户的使用需求。因此出现了如车载智能终端、可穿戴智能终端、智能家居等很多具有融合功能的移动终端。用户在享受其带来的丰富多彩的功能时，却也面临着很多安全风险。近年来，在具有融合功能的移动终端上恶意吸费、隐私泄露等安全事件频发，大大影响到了用户的使用，也制约了其发展。究其原因，融合功能逐渐增多，但是终端设计本身并没有过多的安全考虑，没有适当的安全保护，造成了个人信息泄漏、资费损失等安全问题。因此，有必要对具有融合功能的移动终端的硬件、操作系统、外围接口、应用软件及个人信息保护等方面提出一整套安全要求。

本标准是GB/T 39575—2020配套的测试方法。本标准针对GB/T 39575—2020提出的技术指标设计了相应的、科学的测试方法，用于验证具有融合功能的移动终端是否满足技术要求的规定的内容。通过本标准可加强对具有融合功能的移动终端安全能力的管理，可从测试方法角度保证安全能力要求的实施，切实提高其安全能力。

具有融合功能的移动终端安全能力测试方法

1 范围

本标准规定了具有融合功能的移动终端安全能力的测试方法，包括硬件安全能力、操作系统安全能力、应用软件安全能力、通信连接安全能力、个人信息安全保护能力。

本标准适用于各种制式的具有融合功能的移动终端，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。

GB/T 39575—2020 具有融合功能的移动终端安全能力技术要求

YD/T 3082—2016 移动智能终端上的个人信息保护技术要求

3 术语和定义、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

具有融合功能的移动终端 mobile terminal with syncretic function

可对人或物进行信息采集和处理，具备蜂窝网络和互联网络接入功能，支持语音或数据通信，用于具有融合功能的终端设备。

3.1.2

融合功能 syncretic function

基于终端硬件及软件资源和能力，在终端上承载的除语音和数据通信以外非通信行业功能(例如：数字电视广播、车辆控制、扫码、人体信息采集等)。

3.1.3

脱敏 desensitization

通过模糊化等方法处理原始数据，以实现屏蔽敏感数据且屏蔽后的数据不可逆向恢复的数据保护方式。

3.2 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口(Application Programming Interface)

CNVD：国家信息安全漏洞共享平台(China National Vulnerability Database)

CNNVD：中国国家信息安全漏洞库(China National Vulnerability Database of Information Security)

NFC：近场通信(Near Field Communication)
SD：安全数字存储卡(Secure Digital Memory Card)
USB：通用串行总线(Universal Serial Bus)
WLAN：无线局域网(Wireless Local Area Network)

4 具有融合功能的移动终端安全能力测试方法

4.1 概述

本章描述了针对具有融合功能的移动终端的各种安全能力进行评测的方法。评测结果有以下两种：

——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；
本章所提及的技术要求见 GB/T 39575—2020。

4.2 硬件安全

4.2.1 标识唯一

测试编号：4.2.1
测试项目：标识唯一
项目要求：见 GB/T 39575—2020 中 5.1.1
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：审查厂商提交的文档，查看硬件标识是否可被改写； 步骤 2：尝试改写终端硬件标识信息。
预期结果： 硬件标识唯一且不可改写。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.2.2 设计安全

测试编号：4.2.2
测试项目：设计安全
项目要求：见 GB/T 39575—2020 中 5.1.2
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：审查厂商提交的文档，查看终端硬件芯片接口设计，密钥管理方式； 步骤 2：尝试在未授权条件下调用芯片接口，访问内存； 步骤 3：密钥的生成、分发和存储方式，评估密钥是否存在泄露的风险。

预期结果： 芯片不存在隐蔽调用接口，且访问接口需要经过用户授权； 密钥的产生、分发、使用、存储和销毁采用一定安全机制保护，不存在泄露风险。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.2.3 防止物理攻击

测试编号：4.2.3
测试项目：防止物理攻击
项目要求：见 GB/T 39575—2020 中 5.1.3
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：审查厂商提交的文档，验证厂商声明硬件具有防护非侵入、半侵入和侵入式等物理攻击的能力； 步骤 2：通过实验验证关键硬件具有抵抗旁路攻击、错误注入攻击的能力，旁路攻击包括但不限于简单功耗分析、差分功耗分析、相关功耗分析、电磁辐射分析、模板分析等，错误注入攻击包括但不限于时钟毛刺分析、电压毛刺分析、光信号分析、电磁信号分析等； 步骤 3：评估是否存在信息泄露，包括但不限于密钥、加密数据，评估抵抗物理攻击的能力。
预期结果： 具有融合功能的移动终端硬件具备安全防护机制，不存在泄漏点，无法获得或篡改密钥、加密数据等信息。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.3 系统及软件安全

4.3.1 安全引导

测试编号：4.3.1
测试项目：安全引导
项目要求：见 GB/T 39575—2020 中 5.2.1
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：审查厂商提交的文档，查看被测终端是否具有安全启动机制。评估安全启动过程。
预期结果： 终端采用加密签名，证书链验证等安全引导机制，非授权代码无法执行系统启动。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.3.2 完整性校验

测试编号：4.3.2
测试项目：完整性校验
项目要求：见 GB/T 39575—2020 中 5.2.2
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：审查厂商提交的文档，查看被测终端系统是否具有完整性校验机制； 步骤 2：尝试篡改系统关键代码（包括但不限于系统服务、权限管理、文件校验等），并运行系统。
预期结果： 终端具有完整性校验机制，无法非授权修改关键代码，或篡改后代码无法运行。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.3.3 终端接入认证

测试编号：4.3.3
测试项目：终端接入认证
项目要求：见 GB/T 39575—2020 中 5.2.3
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：审查厂商提交的文档，查看被测终端是否具有接入认证机制； 步骤 2：使用非授权终端尝试接入相关网关或服务器，使用融合功能。
预期结果： 终端具有接入认证机制，且非授权终端无法介入网关或服务器，无法使用融合功能。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.3.4 标识与鉴别

测试编号：4.3.4.1
测试项目：用户标识
项目要求：见 GB/T 39575—2020 中 5.2.4
预置条件：被测移动智能终端处于正常工作状态

测试步骤： 步骤 1：查看终端系统是否有用户标识机制； 步骤 2：模拟操作系统用户进行注册和登录操作，检查标识是否唯一。
预期结果： 凡进入操作系统用户进行了用户表示（建立账号），且表示唯一并与用户名、别名、UID 等一致。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

测试编号：4.3.4.2
测试项目：用户鉴别
项目要求：见 GB/T 39575—2020 中 5.2.4
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：审查厂商提交的文档文档，包括用户鉴别机制实现、存储过程等； 步骤 2：模拟操作系统用户进行登录操作，并执行安全参数设置、口令修改、数据备份等安全功能相关操作。
预期结果： 操作系统要求鉴别用户标识，且在执行安全功能之前执行了用户标识鉴别，且鉴别信息不可见，鉴别信息实现了加密存储。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

测试编号：4.3.4.3
测试项目：鉴别失败处理
项目要求：见 GB/T 39575—2020 中 5.2.4
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：审查厂商提交的文档，是否提供用户鉴别失败处理措施； 步骤 2：模拟用户进行登录操作，并连续鉴别失败，检查系统是否依据预定义鉴别失败处理方法进行了相应的处理。
预期结果： 用户无法登录系统，且系统按照预定规则执行了鉴别失败处理。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.3.5 访问控制

测试编号：4.3.5.1
测试项目：访问控制规则
项目要求：见 GB/T 39575—2020 中 5.2.5
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：审查厂商提交的文档，检查访问控制策略，访问控制属性设置； 步骤 2：尝试使用非授权方式修改访问控制规则。
预期结果： 终端系统有访问控制策略，且访问控制属性至少包括读、写、执行，非授权方式无法修改访问控制策略或采用强制访问控制策略。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

测试编号：4.3.5.2
测试项目：访问控制执行
项目要求：见 GB/T 39575—2020 中 5.2.5
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：模拟操作系统用户尝试本地和远程访问，修改被保护的应用软件、数据。
预期结果： 终端需要用户确认访问过程，且对用户标识进行了鉴别，非授权用户无法访问保护数据。 访问控制策略修改前经过用户鉴别，非授权用户无法更改。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.3.6 权限控制

测试编号：4.3.6
测试项目：权限控制
项目要求：见 GB/T 39575—2020 中 5.2.6
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：审查厂商提交的文档是否可安装应用软件，敏感 API 是否可以被调用； 步骤 2：开发一款软件安装至被测终端，尝试调用敏感 API 接口（包括但不限于拨打电话、发送短信、定位、拍照、录音、访问通讯录）。

预期结果： 终端无法安装除预置软件之外的应用软件； 终端可安装应用软件，且无敏感 API 暴露或提供敏感 API 权限控制策略，控制策略包括允许和拒绝。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.3.7 安全域隔离

测试编号：4.3.7
测试项目：安全域隔离
项目要求：见 GB/T 39575—2020 中 5.2.7
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：审查终端安全策略文档，查看进程、线程、应用软件、用户之间是否采用隔离机制； 步骤 2：尝试访问进程间、应用软件间、用户间隔离数据。
预期结果： 终端提供安全域隔离机制，且隔离数据无法相互访问，或需要访问控制，且访问控制符合系统访问控制策略。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.3.8 日志审计

测试编号：4.3.8.1
测试项目：审计记录
项目要求：见 GB/T 39575—2020 中 5.2.8
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：模拟用户对终端进行连续鉴别、存储耗尽、参数设置、网络访问等操作； 步骤 2：查看终端是否生成审计记录，记录是否包括日期、对象、描述和结果，且日志与实际发生行为一致。
预期结果： 终端可生成审计日志，且日志内容与模拟操作过程一致，日志格式包含日期、对象、描述和结果。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

测试编号：4.3.8.2
测试项目：审计保护
项目要求：见 GB/T 39575—2020 中 5.2.8
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：审查终端是否提供审计保护机制； 步骤 2：使用非授权用户尝试访问审计日志，并尝试修改、删除等操作。
预期结果： 终端提供审计保护机制，非授权用户无法访问审计日志，无法修改和破坏数据。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.3.9 系统安全性

测试编号：4.3.9
测试项目：系统安全性
项目要求：见 GB/T 39575—2020 中 5.2.9
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：审查终端系统、驱动、内核是否含有 CNVD 或 CNNVD 所定义的 6 个月以前的高危及以上漏洞，评估是否会造成重大安全风险。
预期结果： 终端不含有明显的高危及以上漏洞，或漏洞不易利用，安全风险较低。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.3.10 升级更新

测试编号：4.3.10
测试项目：升级更新
项目要求：见 GB/T 39575—2020 中 5.2.10
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：检查操作系统是否提供升级更新能力； 步骤 2：如果提供升级更新能力，使用非授权的操作系统进行更新，并检查终端状态； 步骤 3：使用授权系统进行更新，并检查终端是否在更新前提供备份可选项； 步骤 4：审查更新后安全属性状态。

预期结果： 终端可鉴别系统更新来源，使用非授权系统无法正常更新，系统支持回滚不会出现异常现象；使用授权系统可正常进行更新，且系统更新后数据不会丢失，安全属性与升级前一致。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.3.11 软件安全

4.3.11.1 应用软件来源

测试编号：4.3.11.1
测试项目：应用软件来源
项目要求：见 GB/T 39575—2020 中 5.2.11.1
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：检查操作系统融合功能相关应用软件是否预置在终端内，尝试提取应用软件； 步骤 2：若未预置融合功能相关应用，则通过授权渠道下载安装融合功能相关应用软件； 步骤 3：尝试修改融合功能相关应用软件，再次尝试安装。
预期结果： 终端内预置融合功能相关应用软件，且不可提取，或提取后不可重新安装。 若终端未预置融合功能相关应用软件，则系统可鉴别应用软件来源，并可安装授权渠道获得的应用软件。 修改重打包后的应用软件，无法安装。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.3.11.2 应用软件签名

测试编号：4.3.11.2
测试项目：应用软件签名
项目要求：见 GB/T 39575—2020 中 5.2.11.2
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：检查终端是否提供应用软件签名认证机制； 步骤 2：使用合法签名应用软件安装到终端上； 步骤 3：使用非认证签名应用软件安装到终端上。
预期结果： 终端提供应用软件签名认证机制，经过签名认证的应用软件可以安装到被测终端上，未经认证的应用软件安装时，终端可识别软件状态，禁止软件安装或需要用户确认。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.3.11.3 应用软件安全

测试编号：4.3.11.3
测试项目：应用软件安全
项目要求：见 GB/T 39575—2020 中 5.2.11.3
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：尝试逆向分析终端融合功能相关应用软件、审查代码逻辑、提取用户个人信息、尝试进行反编译、重打包、动态调试等行为。
预期结果： 终端无法提取应用软件，或应用软件支持代码混淆、认证签名、反动态调试等安全机制。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.3.11.4 身份鉴别认证

测试编号：4.3.11.4
测试项目：身份鉴别认证
项目要求：见 GB/T 39575—2020 中 5.2.11.4
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：运行融合功能相关应用软件，检查融合功能使用前是否有登录、认证、密码策略等机制； 步骤 2：检查融合功能是否涉及支付、交易等流程，运行该业务，检查是否有多次认证过程，评估验证手段。
预期结果： 使用融合功能前有登录、认证等机制，且进行高风险业务前，采用了二次认证过程，认证方式包括但不限于短信验证码、动态口令、数字证书、生物识别等方式。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.3.11.5 最小化权限

测试编号：4.3.11.5
测试项目：最小化权限
项目要求：见 GB/T 39575—2020 中 5.2.11.5
预置条件：被测移动智能终端处于正常工作状态

测试步骤： 步骤 1：审查预置应用软件申请的权限，或可以访问的系统资源，包括但不限于个人信息、多媒体数据、系统数据等； 步骤 2：运行应用软件遍历软件功能，检查实际调用接口及访问的系统资源； 步骤 3：审查融合功能相关软件设计方案，采用不同用户登录操作融合功能，审查终端是否按照约定规则对不同用户权限进行了限制。
预期结果： 预置应用软件所申请的权限及访问的资源均在软件合理业务范围内，不存在滥用行为；对不同用户采用了分权管理，用户间不存在权限滥用。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.4 通信连接安全

4.4.1 网络接入安全

测试编号：4.4.1
测试项目：网络接入安全
项目要求：见 GB/T 39575—2020 中 5.3.1
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：审查厂商提交的文档，查看终端是否支持安全协议和融合功能相关协议。
预期结果： 终端支持安全协议实现，支持融合功能协议实现，且安全相关部分符合相应国家或行业标准。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.4.2 外围接口安全

测试编号：4.4.2
测试项目：无线外围接口
项目要求：见 GB/T 39575—2020 中 5.3.2
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：检查终端是否支持 WLAN、蓝牙、NFC、USB、SD 等外围接口； 步骤 2：遍历各个外围接口和物理端口，尝试建立数据连接，并尝试获取业务敏感信息； 步骤 3：尝试接入自启动终端外接存储设备。

预期结果： 终端未包含未声明的外围接口，能够提示用户连接状态，建立数据连接和数据传输前需要用户确认才进行，且未经授权无法获得业务敏感信息，终端闲置物理端口禁用或授权使用，外接存储设备无法自启动。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.4.3 数据传输完整性

测试编号：4.4.3
测试项目：数据传输完整性
项目要求：见 GB/T 39575—2020 中 5.3.3
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：审查厂商提交的文档，检查数据通信过程是否采用完整性保护； 步骤 2：被测终端连接融合功能平台，模拟传输信息数据、通信中断、中间人攻击等过程。
预期结果： 终端采用完整性校验机制，信息无法篡改或经过篡改的信息无法传输，并进行告警等处理，终端包含中断、时延处理机制。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.4.4 数据传输保密性

测试编号：4.4.4
测试项目：数据传输保密性
项目要求：见 GB/T 39575—2020 中 5.3.4
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：审查厂商提交的文档，检查终端采用的加密实现方法； 步骤 2：被测终端连接融合功能平台，采用加密方式模拟传输信息数据； 步骤 3：使用抓包工具，监听传输数据信息。
预期结果： 终端对通信数据提供了加密保护功能，网络包无法还原明文数据，且采用主流加密算法并符合相关行业规定。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.4.5 数据传输健壮性

测试编号:4.4.6
测试项目:数据传输健壮性
项目要求:见 GB/T 39575—2020 中 5.3.6
预置条件:被测移动智能终端处于正常工作状态
测试步骤: 步骤 1:审查厂商提交的文档,检查终端采用的异常处理方法; 步骤 2:被测终端连接融合功能平台,模拟传输信息数据; 步骤 3:终端构造非法信息模拟与平台通信。
预期结果: 终端可识别非法信息,并进行告警、提示、拒绝通信等措施,防止出现异常情况。 若终端满足以上预期结果,则该项目评测结果为“未见异常”,否则为“不符合要求”,评测结束。

4.5 个人信息安全

4.5.1 个人信息采集

测试编号:4.5.1
测试项目:个人信息采集
项目要求:见 GB/T 39575—2020 中 5.4.1
预置条件:被测移动智能终端处于正常工作状态
测试步骤: 步骤 1:审查终端融合功能是否存在收集个人信息的行为,在终端上构造个人信息; 步骤 2:若存在收集个人信息的行为,则判断其是否向用户明示收集目的和范围,且征得了用户同意; 步骤 3:检查终端是否提供数据采集关闭功能。
预期结果: 终端不存在收集个人信息的行为。 若终端存在收集个人信息的行为,则收集前明示用户收集目的和范围,并在收集前经过了用户确认。 终端提供数据采集关闭功能。 若终端满足以上预期结果,则该项目评测结果为“未见异常”,否则为“不符合要求”,评测结束。

4.5.2 个人信息存储

测试编号：4.5.2
测试项目：个人信息存储
项目要求：见 GB/T 39575—2020 中 5.4.2
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：审查终端是否存在本地存储个人信息的行为，在终端上构造个人信息； 步骤 2：若终端存储个人信息，则尝试读取终端个人信息，查看是否有访问控制机制； 步骤 3：采用授权的方式提取账户设置类、传感采集类、金融支付类数据，并查看是否为明文存储。个人信息类型定义见 YD/T 3082—2016。
预期结果： 终端未在本地存储个人信息。 若终端在本地存储个人信息，则终端提供了权限校验、用户鉴别等访问控制机制，未授权用户无法读取个人信息。 账户设置类、传感采集类、金融支付类数据无法提取或为密文存储，无法还原原始数据。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.5.3 个人信息加工

测试编号：4.5.3
测试项目：个人信息加工
项目要求：见 GB/T 39575—2020 中 5.4.3
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：审查终端是否可以修改存储的个人信息，在终端上构造个人信息； 步骤 2：若终端可以修改个人信息，尝试修改终端个人信息，查看是否明示了个人信息的加工目的和范围； 步骤 3：采用授权的方式修改个人信息； 步骤 4：采用非授权的方式修改个人信息； 步骤 5：查看终端传感采集类数据，审查是否采用了脱敏处理。
预期结果： 终端不可修改存储的个人信息。 若终端可以修改个人信息，则在加工前明示了个人信息加工目的和范围，且与实际情况相符，且未授权用户不可修改个人信息。 终端若含有传感采集类数据，则数据采用了抑制、隐藏、泛化、随机化等技术手段进行了脱敏处理。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.5.4 个人信息转移

测试编号：4.5.4
测试项目：个人信息转移
项目要求：见 GB/T 39575—2020 中 5.4.4
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：审查终端是否可以转移个人信息的行为，在终端上构造个人信息； 步骤 2：若终端可以转移个人信息，测尝试转移终端个人信息，查看是否与终端约定目的和用途相同，传输前是否经过双向验证过程； 步骤 3：若终端通过公共网络传输账户设置类、传感采集类、金融支付类个人信息时，则构造非法数据模拟进行传输； 步骤 4：使用抓包工具检查网络传输数据。
预期结果： 终端不可转移个人信息。 若终端可以转移个人信息，则在转移前明示了个人信息转移目的和范围，且与实际情况相符，且转移数据前经过了双方身份认证和授权。 终端若含有账户设置类、传感采集类、金融支付类信息，则非法信息无法送出或接收，且数据采用密文方式。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

4.5.5 个人信息删除

测试编号：4.5.5
测试项目：个人信息删除
项目要求：见 GB/T 39575—2020 中 5.4.5
预置条件：被测移动智能终端处于正常工作状态
测试步骤： 步骤 1：审查终端是否提供删除选项，可删除个人信息； 步骤 2：尝试使用授权用户删除使用记录类、账户设置类、传感采集类、金融支付类信息，并检查删除后终端状态； 步骤 3：尝试恢复传感采集类信息、金融支付类信息，检查信息是否彻底删除。
预期结果： 终端提供给授权用户个人信息删除选项。 若终端授权用户可删除使用记录类、账户设置类、传感采集类、金融支付类信息，且传感采集类信息、金融支付类信息在删除后无法恢复。 若终端满足以上预期结果，则该项目评测结果为“未见异常”，否则为“不符合要求”，评测结束。

参 考 文 献

[1] YD/T 2407 移动智能终端安全能力技术要求
[2] YD/T 2408 移动智能终端安全能力测试方法
[3] YD/T 2674—2013 移动智能终端信息安全设计导则