ICS 35.040
L 80

中华人民共和国国家标准

GB/T 34976—2017

信息安全技术　移动智能终端操作系统安全技术要求和测试评价方法

Information security technology—Security technical requirements and testing and evaluation approaches for operating system of smart mobile terminals

2017-11-01 发布　　2018-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国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。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:公安部第三研究所(公安部计算机信息系统安全产品质量监督检验中心)、中国电子技术标准化研究院、中国信息安全研究院有限公司、上海交通大学、北京元心科技有限公司、上海辰锐信息科技公司、阿里巴巴北京软件服务有限公司、中国信息通信研究院。

本标准主要起草人:张艳、俞优、顾健、陆臻、陈妍、杨晨、许玉娜、沈亮、谷大武、邵旭东、王文杰、白晓媛、姚一楠、顾流。

信息安全技术　移动智能终端操作系统安全技术要求和测试评价方法

1　范围

本标准规定了移动智能终端操作系统的安全技术要求和测试评价方法。

本标准适用于移动智能终端操作系统的生产及测试。

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 18336.3—2015　信息技术　安全技术　信息技术安全评估准则　第3部分：安全保障组件

GB/T 25069—2010　信息安全技术　术语

GB/T 30284—2013　移动通信智能终端操作系统安全技术要求(EAL2级)

3　术语和定义

GB/T 18336.3—2015、GB/T 25069—2010、GB/T 30284—2013界定的以及下列术语和定义适用于本文件。

3.1

移动智能终端　smart mobile terminal

接入移动通信网络、具有操作系统、可由用户自行安装和卸载应用软件的移动通信终端产品。

3.2

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

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

注：一般包括移动智能终端图形交互系统GUI、核心功能库、应用框架、安全套件、业务模型组件、SDK、核心业务功能、基础应用软件等多层架构和软件实体。

3.3

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

移动智能终端操作系统所存储、传输和处理的信息的保密性、完整性和可用性的表征。

4　移动智能终端操作系统安全性描述

移动智能终端操作系统的目的是向用户提供良好的操作界面，便于用户使用移动智能终端的功能。移动智能终端操作系统通过身份鉴别、访问控制、安全审计等安全功能策略，实现对移动智能终端软、硬件的管理，确保移动智能终端的安全运行。其中，硬件包括：通信设备(蜂窝移动通信设备、无线局域网设备)，终端信源传感器(麦克风、摄像头、定位导航系统)，终端输入输出设备(红外接口、蓝牙、USB接口、SDIO接口)等；软件包括存储用户信息的文件(电话号码本、通信记录、短消息、电子邮件、记事本

等)以及相关应用软件。

移动智能终端操作系统保护的资产包括:

——用户数据:包含位置信息、账户信息、通信记录、通讯录等。

——移动智能终端敏感资源:包含通信资源、外设接口,如摄像镜头、位置传感器等。

——移动智能终端操作系统安全功能数据:包含鉴别数据、安全属性等。

此外,移动智能终端操作系统自身的重要数据也是受保护的资产。

5 安全技术要求

5.1 安全功能要求

5.1.1 身份鉴别

5.1.1.1 用户标识

应具备用户标识功能,具体技术要求如下:

a) 凡需进入移动智能终端操作系统的用户,宜先建立用户标识(账号);

b) 仅允许具有用户标识的移动智能终端操作系统用户访问系统安全功能数据等重要数据;

c) 在移动智能终端操作系统的整个生存周期实现用户的唯一性标识,以及用户名或别名、UID等之间的一致性。

5.1.1.2 鉴别技术手段

应具备用户鉴别功能,具体技术要求如下:

a) 在用户执行任何与移动智能终端操作系统安全功能相关的操作之前对用户进行鉴别;

b) 至少支持口令鉴别/基于令牌的动态口令鉴别/生物特征鉴别(如指纹、虹膜)/数字证书鉴别/图形鉴别等机制中的一种进行身份鉴别,并在每次用户登录系统时进行鉴别。

5.1.1.3 鉴别信息保护

应具备鉴别信息保护的能力,具体技术要求如下:

a) 进行用户身份鉴别时,仅将最少的反馈(如:输入的字符数,鉴别的成功或失败)提供给被鉴别的用户;

b) 在用户执行鉴别信息修改操作之前,应经过身份鉴别;

c) 鉴别信息应是不可见的,应采用加密方法对鉴别信息的存储进行安全保护。

5.1.1.4 鉴别失败处理

应通过对不成功的鉴别尝试的值(包括尝试次数和时间的阈值)进行预先定义,并明确规定达到该值时应采取的措施来实现鉴别失败的处理。

5.1.1.5 用户-主体绑定

应具备用户-主体绑定功能,具体技术要求如下:

a) 将用户进程与所有者用户相关联,使用户进程的行为可以追溯到进程的所有者用户;

b) 将系统进程动态地与当前服务要求者用户相关联,使系统进程的行为可以追溯到当前服务的要求者用户。

5.1.2 访问控制

5.1.2.1 访问控制属性

应按以下要求设计和实现访问控制属性：

a) 允许命名用户以用户的身份规定并控制对客体的访问，并阻止非授权用户对客体的访问；

b) 主体的访问控制属性至少应包括：读、写、执行等；

c) 客体的访问控制属性应包含可分配给主体的读、写和执行等权限。

5.1.2.2 访问授权规则

应按以下要求设计和实现访问授权规则：

a) 授权的范围应包括主体和客体及相关的访问控制属性，同时应指出主体和客体对这些规则应用的类型；

b) 对系统中的每一个客体，都应能够实现由客体的创建者以用户指定方式确定其对该客体的访问权限；

c) 客体的拥有者对其拥有的客体应具有全部控制权，允许客体拥有者把该客体的控制权分配给其他主体。

5.1.3 安全审计

5.1.3.1 审计内容

应对与移动智能终端操作系统安全相关的以下事件生成审计日志：系统运行记录、报警记录、操作日志、网络流量记录、用户行为记录、应用软件运行日志、配置信息等；审计日志的内容至少应包括事件发生的日期、时间、主体标识、事件类型描述和结果（成功或失败）、关联的进程。

5.1.3.2 审计保护

应按以下要求设计和实现访问审计保护能力：

a) 能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏；

b) 提供授权管理员一个受保护的打开和关闭审计的机制，该机制能选择和改变审计事件，并在系统工作时处于默认状态；

c) 仅允许授权管理员访问审计日志。

5.1.3.3 审计跟踪管理

应按以下要求设计和实现审计跟踪管理：

a) 操作系统用户应能够定义审计跟踪的阈值；

b) 当为审计系统分配的存储空间耗尽时，应能按操作系统用户的设置决定采取的措施，包括：报警并丢弃未记录的审计信息、暂停审计、覆盖以前的审计记录等。

5.1.4 用户数据安全

5.1.4.1 用户数据保护

应按以下要求设计和实现用户数据保护：

a) 保证用户数据不被未授权查阅或修改；

b) 对应用软件获取用户数据行为进行自动分析、告警和阻断。

5.1.4.2 用户数据完整性

应提供移动智能终端操作系统用户数据在存储和处理过程中的完整性保护。

5.1.4.3 用户数据保密性

应对用户敏感数据采用一定强度的加密储存或采用隐藏技术，以减小移动终端丢失所造成的损失。

5.1.4.4 剩余信息保护

应按以下要求设计和实现剩余信息保护：

a) 确保非授权用户不能查找使用后返还系统的存储介质中的信息内容；
b) 确保非授权用户不能查找系统现已分配给其的存储介质中以前的信息内容。

5.1.5 数据安全

应按以下要求设计和实现数据安全保护能力：

a) 对重要的系统数据（如配置和控制信息、告警和事件数据等）进行存储保护，保证重要系统数据不被泄漏或篡改；
b) 具有用户数据、系统数据的安全备份与恢复功能；
c) 在数据的存储空间达到阈值时能够向移动智能终端操作系统用户进行报警；
d) 当存储空间将要耗尽时，采取一定措施保证重要的数据不丢失。

5.1.6 存储介质管理

应按以下要求设计和实现存储介质管理：

a) 对移动智能终端中的存储设备（包括智能芯片、存储卡等）进行有效监测和统一管理；
b) 在单用户系统中，系统应防止用户进程影响系统的运行；
c) 在多用户系统中，系统应确保多用户间采取一定隔离机制，防止用户数据的非授权访问；
d) 在多系统情况下，应确保多系统间采取一定隔离机制，防止系统数据的非授权访问。

5.1.7 应用软件安全管理

应对第三方应用程序的安装、运行、卸载进行安全规范：

a) 支持用户对应用软件的安装进行授权或阻止；
b) 支持用户修改、指定应用软件的安装位置；
c) 支持用户对应用软件使用的终端资源（包含通信资源和外设接口）和终端数据进行确认；
d) 在应用软件卸载时删除由其生成的资源文件、配置文件和用户数据。

5.1.8 用户策略管理

应提供以下用户策略管理：

a) 对移动智能终端用户提供初始化策略；
b) 支持授权用户对用户策略的添加、删除、修改操作；
c) 支持用户策略查询、导入、导出策略等操作。

5.1.9 运行安全保护

应提供以下运行安全保护：

a) 系统在设计时不应以维护、支持或操作需要为借口，设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口；

b) 将移动智能终端操作系统程序与用户程序进行隔离；
c) 防止在用户模式下运行的进程对系统段进行写操作，而在系统模式下运行时，应允许进程对所有的虚存空间进行读、写操作。

5.1.10 升级能力

应提供以下升级能力：
a) 支持操作系统的更新升级；
b) 至少采取一种安全机制，保证升级过程的安全性；
c) 保证升级后前的系统安全属性与升级前保持一致；
d) 在升级失败时，系统应能够回滚，并保证系统完整性，且安全属性与升级前一致；
e) 至少采取一种安全机制，保证升级的时效性，例如自动升级，更新通知等手段；
f) 支持用户获取、统一管理并运用补丁对移动智能终端操作系统的漏洞进行修补。

5.1.11 超时锁定或注销

应按以下要求设计和实现超时处理能力：
a) 具有登录超时锁定或注销功能；
b) 提供用户设定最大超时时间的功能；
c) 在设定的时间段内没有任何操作的情况下，终止会话，需要再次进行身份鉴别才能够重新操作；
d) 提供用户主动锁定或注销的功能。

5.1.12 运行监控

应提供对移动智能终端设备运行状态（比如 CPU 使用率、内存占用率、存储空间等）、网络连接、系统环境、敏感数据访问状态、敏感功能使用状态的监测。

5.1.13 可靠时钟

应提供手工设定系统时钟和远程时钟服务自动时钟同步两种方式的系统时钟设置功能。

5.1.14 可用性

5.1.14.1 稳定性

正常工作状态下，移动智能终端操作系统应能稳定运行，功耗低、内存占用少，不应造成移动智能终端死机现象。

5.1.14.2 兼容性

应按以下要求设计和实现兼容性：
a) 除了自带的应用程序，移动智能终端操作系统应提供良好的第三方软件应用接口，能够支持第三方应用软件的安装、运行和升级功能；
b) 具备无线接入互联网的能力。

5.2 安全保障要求

5.2.1 开发

5.2.1.1 安全架构

开发者应提供终端操作系统安全功能的安全架构描述，安全架构描述应满足以下要求：

a) 与产品设计文档中对安全功能实施抽象描述的级别一致；
b) 描述与安全功能要求一致的终端操作系统安全功能的安全域；
c) 描述终端操作系统安全功能初始化过程为何是安全的；
d) 证实终端操作系统安全功能能够防止被破坏；
e) 证实终端操作系统安全功能能够防止安全特性被旁路。

5.2.1.2 功能规范

开发者应提供完备的功能规范说明，功能规范说明应满足以下要求：
a) 完全描述终端操作系统的安全功能；
b) 描述所有安全功能接口的目的与使用方法；
c) 标识和描述每个安全功能接口相关的所有参数；
d) 描述安全功能接口相关的安全功能实施行为；
e) 描述由安全功能实施行为处理而引起的直接错误消息；
f) 证实安全功能要求到安全功能接口的追溯。

5.2.1.3 产品设计

开发者应提供产品设计文档，产品设计文档应满足以下要求：
a) 根据子系统描述终端操作系统结构；
b) 标识和描述终端操作系统安全功能的所有子系统；
c) 描述安全功能所有子系统间的相互作用；
d) 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的安全功能接口。

5.2.2 指导性文档

5.2.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述应满足以下要求：
a) 描述在安全处理环境中被控制的用户可访问的功能和特权，包含适当的警示信息；
b) 描述如何以安全的方式使用终端操作系统提供的可用接口；
c) 描述可用功能和接口，尤其是受用户控制的所有安全参数，适当时指明安全值；
d) 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变安全功能所控制实体的安全特性；
e) 标识终端操作系统运行的所有可能状态(包括操作导致的失败或者操作性错误)，以及它们与维持安全运行之间的因果关系和联系；
f) 充分实现安全目的所执行的安全策略。

5.2.2.2 准备程序

开发者应提供终端操作系统及其准备程序，准备程序描述应满足以下要求：
a) 描述与开发者交付程序相一致的安全接收所交付终端操作系统必需的所有步骤；
b) 描述安全安装终端操作系统及其运行环境必需的所有步骤。

5.2.3 生命周期支持

5.2.3.1 配置管理能力

开发者的配置管理能力应满足以下要求：

a) 为终端操作系统的不同版本提供唯一的标识；
b) 使用配置管理系统对组成终端操作系统的所有配置项进行维护，并唯一标识配置项；
c) 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法。

5.2.3.2 配置管理范围

开发者应提供终端操作系统配置项列表，并说明配置项的开发者。配置项列表至少包含终端操作系统、安全保障要求的评估证据和终端操作系统的组成部分。

5.2.3.3 交付程序

开发者应使用一定的交付程序交付终端操作系统，并将交付过程文档化。在给用户方交付终端操作系统的各版本时，交付文档应描述为维护安全所必需的所有程序。

5.2.4 测试

5.2.4.1 覆盖

开发者应提供测试覆盖文档，测试覆盖描述应表明测试文档中所标识的测试与功能规范中所描述的终端操作系统的安全功能间的对应性。

5.2.4.2 功能测试

开发者应测试终端操作系统安全功能，将结果文档化并提供测试文档。测试文档应包括以下内容：
a) 测试计划，标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其他测试结果的任何顺序依赖性；
b) 预期的测试结果，表明测试成功后的预期输出；
c) 实际测试结果和预期的测试结果一致。

5.2.4.3 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源，以用于安全功能的抽样测试。

5.2.5 脆弱性评定

开发者应执行脆弱性分析，并提供脆弱性分析文档。基于已标识的潜在脆弱性，终端操作系统能够抵抗具有基本攻击潜力攻击者的攻击。

6 测试评价方法

6.1 安全功能要求测试

6.1.1 身份鉴别

6.1.1.1 用户标识

用户标识的测试评价方法如下：
a) 测试方法：
模拟移动智能终端操作系统用户进行注册和登录操作，检查用户标识是否唯一。
b) 预期结果：
记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

1） 凡需进入移动智能终端操作系统的用户，应先进行用户标识（建立账号）；
2） 应在移动智能终端操作系统的整个生存周期实现用户的唯一性标识，以及用户名或别名、UID 等之间的一致性。

c） 结果判定：
上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.1.2 鉴别技术手段

鉴别技术手段的测试评价方法如下：

a） 测试方法：
1） 模拟移动智能终端操作系统用户进行登录操作，并执行安全参数配置、口令修改、数据备份等安全功能相关操作，检查用户在执行任何与移动智能终端操作系统安全功能相关的操作之前是否进行鉴别；
2） 检查移动智能终端操作系统提供的用户鉴别机制是否包括提供用户名、口令方式；
3） 查看移动智能终端操作系统是否提供其他用户鉴别机制，如基于令牌的动态口令鉴别/生物特征鉴别（如指纹、虹膜）/数字证书等。

b） 预期结果：
记录测试结果并对该结果是否完全符合上述测试预期结果要求作出判断，应符合：
1） 应在用户执行任何与移动智能终端操作系统功能相关的操作之前至少使用一种鉴别机制进行用户合法性鉴别；
2） 应至少提供以下鉴别机制中的一种方式进行身份鉴别：口令鉴别/基于令牌的动态口令鉴别/生物特征鉴别（如指纹、虹膜）/数字证书鉴别等，并在每次用户登录系统时进行鉴别。

c） 结果判定：
上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.1.3 鉴别信息保护

鉴别信息保护的测试评价方法如下：

a） 测试方法：
1） 模拟用户进行移动智能终端操作系统登录操作，如输入口令、指纹信息等；
2） 模拟用户执行鉴别信息修改操作，查看系统是否要求进行用户身份鉴别；
3） 根据产品资料确定鉴别信息存放路径，分别尝试以授权和非授权的方式读取用户的账号、口令密码信息。

b） 预期结果：
1） 若进行身份鉴别时，用户口令明文显示，则本项判为不合格；
2） 若用户鉴别信息修改操作之前，无需进行身份鉴别，则本项判为不合格；
3） 若以授权方式或非授权方式能够获得以上鉴别信息的明文内容，则本项判为不合格。

c） 结果判定：
上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.1.4 鉴别失败处理

鉴别失败处理的测试评价方法如下：

a） 测试方法：
1） 检查系统是否提供用户鉴别失败处理措施；
2） 对不成功的鉴别尝试的值（包括尝试次数和时间的阈值）及鉴别失败处理措施进行参数设置；

3） 模拟移动智能终端操作系统用户进行登录操作，并连续鉴别失败，检查系统是否依据鉴别失败处理措施的参数配置进行相应处理。

b） 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

应通过对不成功的鉴别尝试的值（包括尝试次数和时间的阈值）进行预先定义，并明确规定达到该值时应采取的措施来实现鉴别失败的处理。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.1.5 用户-主体绑定

用户-主体绑定的测试评价方法如下：

a） 测试方法：

1） 检查系统是否提供将用户进程与所有者用户相关联的用户主体绑定功能，使用户进程的行为可以追溯到进程的所有者用户；

2） 检查系统是否提供将系统进程动态地与当前服务要求者用户相关联的用户主体绑定功能，使系统进程的行为可以追溯到当前服务的要求者用户。

b） 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

1） 将用户进程与所有者用户相关联，使用户进程的行为可以追溯到进程的所有者用户；

2） 将系统进程动态地与当前服务要求者用户相关联，使系统进程的行为可以追溯到当前服务的要求者用户。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.2 访问控制

6.1.2.1 访问控制属性

访问控制属性的测试评价方法如下：

a） 测试方法：

1） 检查系统是否提供访问控制机制，允许用户规定并控制对客体的访问；

2） 检查系统提供的访问控制机制是否阻止非授权用户对客体的访问；

3） 检查系统提供主体的访问控制属性，是否包括读、写、执行等；

4） 检查系统提供客体的访问控制属性，是否包括可分配给主体的读、写和执行等权限。

b） 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

1） 允许命名用户以用户的身份规定并控制对客体的访问，并阻止非授权用户对客体的访问；

2） 主体的访问控制属性至少应有：读、写、执行等；客体的访问控制属性应包含可分配给主体的读、写和执行等权限。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.2.2 访问授权规则

访问授权规则的测试评价方法如下：

a) 测试方法：

1) 检查系统是否提供访问授权规则；

2) 查看系统提供访问授权规则的授权范围，是否包括主体和客体及相关的访问控制属性，并指出主体和客体对这些规则应用的类型；

3) 查看系统提供访问授权规则的授权范围，是否覆盖了系统中的每一个客体，并由客体的创建者以用户指定方式确定其对该客体的访问权限；

4) 检查系统中客体的拥有者是否拥有该客体的全部控制权，并允许该客体拥有者把该客体的控制权分配给其他主体。

b) 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

1) 授权的范围应包括主体和客体及相关的访问控制属性，同时应指出主体和客体对这些规则应用的类型；

2) 对系统中的每一个客体，都应能够实现由客体的创建者以用户指定方式确定其对该客体的访问权限；

3) 客体的拥有者对其拥有的客体应具有全部控制权，允许客体拥有者把该客体的控制权分配给其他主体。

c) 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.3 安全审计

6.1.3.1 审计内容

审计内容的测试评价方法如下：

a) 测试方法：

1) 模拟用户对移动智能终端进行连续鉴别失败、数据存储空间耗尽、参数设置、网络访问等操作；

2) 查看审计日志，检查审计数据是否包括系统运行记录、报警记录、操作日志、网络流量记录、用户行为记录、应用软件运行日志、配置信息等；

3) 检查日志项是否包括了事件发生的日期和时间、触发事件的主体、事件的类型、事件成功或失败等。

b) 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

1) 应能够获取各种类型安全事件的审计数据，如：系统运行记录、报警记录、操作日志、网络流量记录、用户行为记录、应用软件运行日志、配置信息等；

2) 每个事件的审计记录，应包括以下信息：事件发生的日期和时间、触发事件的用户或进程主体、事件的类型、事件成功或失败等。

c) 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.3.2 审计保护

审计保护的测试评价方法如下：

a) 测试方法：

1) 检测系统是否提供对审计功能的保护措施，限制未授权用户对审计记录的访问；

2） 检测系统是否提供用户打开和关闭审计的机制；

3） 模拟用户对审计功能进行打开/关闭操作，重启系统，查看系统是否根据用户设置提供默认的审计机制。

b） 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

1） 能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏，特别要保护审计数据，要严格限制未经授权的用户访问；

2） 应提供用户一个受保护的打开和关闭审计的机制，该机制能选择和改变审计事件，并在系统工作时处于默认状态。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.3.3 审计跟踪管理

审计跟踪管理的测试评价方法如下：

a） 测试方法：

1） 检测系统是否提供审计存储空间维护功能；

2） 模拟操作系统用户设置审计跟踪极限的阈值；

3） 当存储空间被耗尽时，检测系统是否依据设定的阈值，按操作系统用户的设置提供指定的措施，如报警并丢弃未记录的审计信息、暂停审计、覆盖以前的审计记录等。

b） 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

1） 操作系统用户应能够定义超过审计跟踪极限的阈值；

2） 当存储空间被耗尽时，应能按操作系统用户的指定决定采取的措施，包括：报警并丢弃未记录的审计信息、暂停审计、覆盖以前的审计记录等。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.4 用户数据安全

6.1.4.1 用户数据保护

用户数据保护的测试评价方法如下：

a） 测试方法：

1） 模拟非授权用户尝试对用户数据进行查阅和修改，检测系统能否限制类似非授权行为；

2） 检测系统能否对应用软件获取用户数据的行为进行自动分析、告警和阻断。

b） 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

1） 产品应保证用户数据不被未授权查阅或修改；

2） 对应用软件获取用户数据行为进行自动分析、告警和阻断。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.4.2 用户数据完整性

用户数据完整性的测试评价方法如下：

a） 测试方法：

分别对用户数据在存储、传输和处理过程中进行完整性破坏，检测系统是否提供用户数据在存储和处理过程中的完整性保护措施。

b） 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

应提供移动智能终端操作系统用户数据在存储和处理过程中的完整性保护。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.4.3 用户数据保密性

用户数据保密性的测试评价方法如下：

a） 测试方法：

检测系统是否对用户敏感数据（如各类账号、口令、定位信息、通讯录、短信、照片等）采用加密存储或隐藏技术。

b） 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

用户敏感数据应采用一定强度的加密储存或采用隐藏技术，以减小移动终端丢失所造成的损失。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.4.4 剩余信息保护

剩余信息保护的测试评价方法如下：

a） 测试方法：

检测系统是否提供剩余信息保护功能，以确保非授权用户无法查找系统现已分配给其的存储介质中以前的信息内容，以及使用后返还系统的存储介质中的信息内容。

b） 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

1） 应确保非授权用户不能查找使用后返还系统的存储介质中的信息内容；

2） 应确保非授权用户不能查找系统现已分配给其的存储介质中以前的信息内容。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.5 数据安全

数据安全的测试评价方法如下：

a） 测试方法：

1） 检测系统是否采用访问控制、加密等机制，提供对重要的系统数据（如配置和控制信息、告警和事件数据等）的安全保护措施；

2） 检测系统是否具备对日常数据安全备份与恢复功能，模拟系统用户进行数据备份和恢复操作，验证该项功能的有效性；

3） 模拟系统用户设置数据存储空间阈值参数，当数据的存储空间达到阈值时，检测系统能否向系统用户进行自动报警；

4） 查看系统在存储空间将要耗尽时，是否提供相应措施保证未及时保存的数据不丢失。

b） 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

1） 应提供有效、合理、安全的数据存储方案，对重要的系统数据（如配置和控制信息、告警和事件数据等）进行存储保护，保证重要系统数据不被泄漏或篡改；

2） 应具有日常数据安全备份与恢复功能；

3） 应在数据的存储空间达到阈值时能够向移动智能终端操作系统用户进行报警；

4） 当存储空间将要耗尽时，应采取一定措施保证从数据源传来的未及时保存的数据不丢失。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.6 存储介质管理

存储介质管理的测试评价方法如下：

a） 测试方法：

1） 检测系统是否提供对移动智能终端中的存储设备（包括智能芯片、存储卡等）的统一管理和检测功能；

2） 在多用户系统中，分别模拟不同用户 A、用户 B 登录操作系统，操作终端并各自生成用户数据存储于存储介质上，尝试以用户 A 非授权访问存储介质中由用户 B 生成的用户数据，查看是否能否访问成功。

b） 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

1） 可对移动智能终端中的存储设备（包括智能芯片、存储卡等）进行有效监测和统一管理；

2） 在单用户系统中，应防止用户进程影响系统的运行；

3） 在多用户系统中，系统对多用户间采取一定隔离机制，用户无法非授权访问其他用户的数据。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.7 应用软件安全管理

应用软件安全管理的测试评价方法如下：

a） 测试方法：

1） 在移动智能终端上安装终端应用软件，检查是否提示用户对应用软件的安装进行授权；

2） 检查用户是否能够修改默认安装位置，并设置应用软件的安装位置；

3） 检查用户是否能够对应用软件使用的终端资源（如网络通信模块、摄像头、导航定位等）和终端数据（如相册、通讯录等）进行确认；

4） 卸载终端应用软件，检查其安装及使用生成的数据是否被完全删除。

b） 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

1） 系统依据用户对应用软件的安装授权正确在移动智能终端上安装应用软件，并生成相应图标；

2） 安装位置可由终端操作系统用户指定；

3） 提示终端操作系统用户对其使用的终端资源和终端数据进行确认；

4） 终端应用软件安装后，终端操作系统和其他应用软件仍能正常使用；

5） 卸载时能够将其安装及使用过程产生的资源文件、配置文件和用户数据全部删除。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.8 用户策略管理

用户策略管理的测试评价方法如下：

a） 测试方法：

1） 检测系统是否为系统用户提供了初始化策略；

2） 模拟用户对于策略进行添加、删除、修改、查询、导入、导出等操作，查看能否操作成功。

b） 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

1） 应对移动智能终端用户提供初始化策略；

2） 支持授权用户对用户策略的添加、删除、修改操作；

3） 支持用户策略分发、查询、导入、导出策略等操作。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.9 运行安全保护

运行安全保护的测试评价方法如下：

a） 测试方法：

1） 查看操作系统设计文档，检查系统设计时是否有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口；

2） 查看操作系统设计文档，检查系统是否将系统程序与用户程序进行隔离。

b） 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

1） 系统在设计时不应以维护、支持或操作需要为借口，设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口；

2） 应将移动智能终端操作系统程序与用户程序进行隔离；

3） 应防止在用户模式下运行的进程对系统段进行写操作；而在系统模式下运行时，应允许进程对所有的虚存空间进行读、写操作。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.10 升级能力

升级能力的测试评价方法如下：

a） 测试方法：

1） 检查产品的升级更新方式，进行相应策略配置，验证升级功能的有效性；

2） 检查产品的升级频率，验证升级功能的及时性；

3） 对系统进行安全属性配置后进行升级更新操作，查看升级后的系统安全属性是否与升级前一致；

4） 在系统更新升级过程中，通过断网、关机等操作导致升级失败，查看系统是否具备回滚机制，确保系统安全属性与升级操作前一致；

5） 对升级包进行篡改，检查产品能否升级成功。

b） 预期结果：

1） 系统应具有及时更新、升级功能，并确保升级前后的系统安全属性一致性；

2） 系统应通过签名验证等机制确保升级包的完整性。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.11 超时锁定或注销

超时锁定或注销的测试评价方法如下：

a） 测试方法：

1） 检测系统是否提供用户登录超时锁定或注销功能；

2） 模拟系统用户设置最大超时时间阈值，并在设定的时间段内没有任何操作，检测系统能否终止用户会话，检测用户是否需进行身份鉴别后才能继续系统操作。

b） 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

1） 应具有登录超时锁定或注销功能；

2） 应提供用户设定最大超时时间的功能；

3） 在设定的时间段内没有任何操作的情况下，终止会话，需要再次进行身份鉴别才能够重新操作。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.12 运行监控

运行监控的测试评价方法如下：

a） 测试方法：

检测系统是否提供对移动智能终端设备运行状态（比如 CPU 使用率、内存占用率、存储空间等）、网络连接、系统环境的状态实时监测。

b） 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

应提供对移动智能终端设备运行状态（比如 CPU 使用率、内存占用率、存储空间等）、网络连接、系统环境的监测。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.13 可靠时钟

可靠时钟的测试评价方法如下：

a） 测试方法：

1） 检测系统是否提供手工、自动时钟设置功能；

2） 手动更改系统日期和时间，查看界面显示日期和时间是否更新为所设日期和时间；

3） 选择自动设置日期和时间，查看界面显示时间是否更新为当前实际日期和时间；

4） 手动更改系统时区，查看界面显示系统时区是否更新。

b） 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

应提供手工设定系统时钟和远程时钟服务自动时钟同步两种方式的系统时钟设置功能。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.14 可用性

6.1.14.1 稳定性

稳定性的测试评价方法如下：

a） 测试方法：

模拟用户在智能终端上部署并使用操作系统，进行各种功能操作。

b） 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

1） 产品在智能终端正常工作状态下应工作稳定，不应造成移动智能终端死机现象；

2） 产品的运行不应影响移动智能终端的正常网络通信。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.1.14.2 兼容性

兼容性的测试评价方法如下：

a） 测试方法：

1） 检测系统是否提供了第三方软件应用接口；

2） 模拟用户在操作系统上安装并使用第三方应用软件，并进行软件升级操作。

b） 预期结果：

记录测试结果并对该结果是否完全符合上述测试方法要求作出判断，应符合：

1） 除了自带的应用程序，移动智能终端操作系统应提供良好的第三方软件应用接口；

2） 能够支持第三方应用软件的安装、运行和升级功能。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.2 安全保障要求测试

6.2.1 开发

6.2.1.1 安全架构

安全架构的测试评价方法如下：

a） 测试方法：

审查安全架构文档是否准确描述如下内容：

1） 与产品设计文档中对安全功能实施抽象描述的级别一致；

2） 描述与安全功能要求一致的终端操作系统安全功能的安全域；

3） 描述终端操作系统安全功能初始化过程为何是安全的；

4） 证实终端操作系统安全功能能够防止被破坏；

5） 证实终端操作系统安全功能能够防止安全特性被旁路。

b） 预期结果：

开发者提供的文档内容应满足上述要求。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.2.1.2 功能规范

功能规范的测试评价方法如下：

a) 测试方法：

审查功能规范文档是否准确描述如下内容：

1) 完全描述终端操作系统的安全功能；
2) 描述所有安全功能接口的目的与使用方法；
3) 标识和描述每个安全功能接口相关的所有参数；
4) 描述安全功能接口相关的安全功能实施行为；
5) 描述由安全功能实施行为处理而引起的直接错误消息；
6) 证实安全功能要求到安全功能接口的追溯。

b) 预期结果：

开发者提供的文档内容应满足上述要求。

c) 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.2.1.3 产品设计

产品设计的测试评价方法如下：

a) 测试方法：

审查产品设计文档是否准确描述如下内容：

1) 根据子系统描述终端操作系统结构；
2) 标识和描述终端操作系统安全功能的所有子系统；
3) 描述安全功能所有子系统间的相互作用；
4) 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的安全功能接口。

b) 预期结果：

开发者提供的文档内容应满足上述要求。

c) 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.2.2 指导性文档

6.2.2.1 操作用户指南

操作用户指南的测试评价方法如下：

a) 测试方法：

审查操作用户指南是否准确描述如下内容：

1) 描述在安全处理环境中被控制的用户可访问的功能和特权，包含适当的警示信息；
2) 描述如何以安全的方式使用终端操作系统提供的可用接口；
3) 描述可用功能和接口，尤其是受用户控制的所有安全参数，适当时指明安全值；
4) 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变安全功能所控制实体的安全特性；
5) 标识终端操作系统运行的所有可能状态(包括操作导致的失败或者操作性错误)，以及它们与维持安全运行之间的因果关系和联系；

6） 充分实现安全目的所执行的安全策略。

b） 预期结果：

开发者提供的文档内容应满足上述要求。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.2.2.2 准备程序

准备程序的测试评价方法如下：

a） 测试方法：

审查准备程序文档是否准确描述如下内容：

1） 描述与开发者交付程序相一致的安全接收所交付终端操作系统必需的所有步骤；

2） 描述安全安装终端操作系统及其运行环境必需的所有步骤。

b） 预期结果：

开发者提供的文档内容应满足上述要求。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.2.3 生命周期支持

6.2.3.1 配置管理能力

配置管理能力的测试评价方法如下：

a） 测试方法：

1） 审查开发者是否为不同版本的终端操作系统提供唯一的标识；

2） 现场检查配置管理系统是否对所有的配置项作出唯一的标识，且配置管理系统是否对配置项进行了维护；

3） 审查开发者提供的配置管理文档，是否描述了对配置项进行唯一标识的方法。

b） 预期结果：

开发者提供的文档和现场活动证据内容应满足上述要求。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.2.3.2 配置管理范围

配置管理范围的测试评价方法如下：

a） 测试方法：

1） 审查开发者提供的配置项列表；

2） 配置项列表是否描述了组成终端操作系统的全部配置项及相应的开发者。

b） 预期结果：

开发者提供的文档和现场活动证据内容应满足上述要求。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.2.3.3 交付程序

交付程序的测试评价方法如下：

a) 测试方法：

1) 现场检查开发者是否使用一定的交付程序交付终端操作系统；

2) 审查开发者是否使用文档描述交付过程，文档中是否包含以下内容：在给用户方交付系统的各版本时，为维护安全所必需的所有程序。

b) 预期结果：

开发者提供的文档和现场活动证据内容应满足上述要求。

c) 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.2.4 测试

6.2.4.1 覆盖

覆盖的测试评价方法如下：

a) 测试方法：

审查开发者提供的测试覆盖文档，在测试覆盖证据中，是否表明测试文档中所标识的测试与功能规范中所描述的终端操作系统的安全功能是对应的。

b) 预期结果：

开发者提供的文档内容应满足上述要求。

c) 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.2.4.2 功能测试

功能测试的测试评价方法如下：

a) 测试方法：

1) 审查开发者提供的测试文档，是否包括测试计划、预期的测试结果和实际测试结果；

2) 审查测试计划是否标识了要测试的安全功能，是否描述了每个安全功能的测试方案（包括对其他测试结果的顺序依赖性）；

3) 审查期望的测试结果是否表明测试成功后的预期输出；

4) 审查实际测试结果是否表明每个被测试的安全功能能按照规定进行运作。

b) 预期结果：

开发者提供的文档内容应满足上述要求。

c) 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.2.4.3 独立测试

独立测试的测试评价方法如下：

a) 测试方法：

1) 评价者应审查开发者提供的测试资源；

2) 评价者应抽查并测试开发者提供的测试集合是否与其自测系统功能时使用的测试集合相一致。

b) 预期结果：

开发者提供的资源应满足上述要求。

c) 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6.2.5 脆弱性评定

脆弱性评定的测试评价方法如下：

a） 测试方法：

1） 审查开发者提供的脆弱性分析文档，是否对所标识的每个具有安全功能强度声明的安全机制进行了安全功能强度分析；

2） 从用户可能破坏安全策略的明显途径出发，按照安全机制定义的安全强度级别，对终端操作系统进行脆弱性分析；

3） 利用相关工具、脚本及人工渗透测试方法，参照 CNNVD 等权威漏洞发布平台公布的高中危漏洞，对被测操作系统进行攻击测试和漏洞验证。

b） 预期结果：

渗透性测试结果应表明终端操作系统能够抵抗具有基本攻击潜力攻击者的攻击。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。