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 …… Ⅲ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　移动智能终端操作系统安全性描述 …… 1
5　安全技术要求 …… 2
5.1　安全功能要求 …… 2
5.1.1　身份鉴别 …… 2
5.1.2　访问控制 …… 3
5.1.3　安全审计 …… 3
5.1.4　用户数据安全 …… 3
5.1.5　数据安全 …… 4
5.1.6　存储介质管理 …… 4
5.1.7　应用软件安全管理 …… 4
5.1.8　用户策略管理 …… 4
5.1.9　运行安全保护 …… 4
5.1.10　升级能力 …… 5
5.1.11　超时锁定或注销 …… 5
5.1.12　运行监控 …… 5
5.1.13　可靠时钟 …… 5
5.1.14　可用性 …… 5
5.2　安全保障要求 …… 5
5.2.1　开发 …… 5
5.2.2　指导性文档 …… 6
5.2.3　生命周期支持 …… 6
5.2.4　测试 …… 7
5.2.5　脆弱性评定 …… 7
6　测试评价方法 …… 7
6.1　安全功能要求测试 …… 7
6.1.1　身份鉴别 …… 7
6.1.2　访问控制 …… 9
6.1.3　安全审计 …… 10
6.1.4　用户数据安全 …… 11
6.1.5　数据安全 …… 12
6.1.6　存储介质管理 …… 13
6.1.7　应用软件安全管理 …… 13
6.1.8　用户策略管理 …… 14

6.1.9 运行安全保护 …… 14
6.1.10 升级能力 …… 14
6.1.11 超时锁定或注销 …… 15
6.1.12 运行监控 …… 15
6.1.13 可靠时钟 …… 15
6.1.14 可用性 …… 16
6.2 安全保障要求测试 …… 16
6.2.1 开发 …… 16
6.2.2 指导性文档 …… 17
6.2.3 生命周期支持 …… 18
6.2.4 测试 …… 19
6.2.5 脆弱性评定 …… 20

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