ICS 35.040
L 80

中华人民共和国国家标准

GB/T 30284—2020
代替 GB/T 30284—2013

信息安全技术　移动通信智能终端操作系统安全技术要求

**Information security techniques—
Security technical requirements for operating system on smart mobile terminal**

2020-04-28 发布　　2020-11-01 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。

本标准代替 GB/T 30284—2013《移动通信智能终端操作系统安全技术要求(EAL2 级)》。

本标准与 GB/T 30284—2013 相比,主要技术变化如下:

——修改了标准名称为《信息安全技术　移动通信智能终端操作系统安全技术要求》;

——修改了“范围”中安全技术要求级别(见第 1 章);

——修改了第 2 章规范性引用文件(见第 2 章和 2013 年版的第 2 章);

——增加了术语“可信信道”“可信路径”和“TSF 数据”及其定义(见 3.1.9、3.1.10、3.1.11);

——修改了术语“移动通信智能终端”和“用户数据”的定义(见 3.1.7、3.1.12);

——删除了部分术语(见 2013 年版的第 3 章);

——增加了部分缩略语(见 3.2);

——修改了移动通信智能终端操作系统描述(见 4.1);

——修改了安全问题定义中“威胁”“组织安全策略”和“假设”的规定(见 5.2、5.3、5.4);

——修改了安全目的的规定(见第 6 章);

——将原标准第 7 章“安全功能要求”和第 8 章“安全保障要求”合并为 “安全要求”(见第 7 章);

——删除了“安全审计类:FAU”中的“审计查阅(FAU_SAR.1)”和“有限审计查阅(FAU_SAR.2)”(见 2013 年版的 7.9.4 和 7.9.5);

——删除了“密码支持类:FCS”中的扩展组件“密码支持基本要求(FCS_CBR_EXT.1)”和“密码操作应用(FCS_COA_EXT.1)”(见 2013 年版的 7.7.2 和 7.7.3);

——删除了“安全管理类:FMT”中的“安全属性撤销(FMT_REV.1)” (见 2013 年版的 7.5.10);

——删除了“TOE 访问类:FTA”中“TOE 会话建立(FTA_TSE.1)”和“可选属性范围限定(FTA_LSA.1)”(见 2013 年版的 7.6.4 和 7.6.5);

——增加了“安全审计(FAU 类)”中的“防止审计数据丢失(FAU_STG.4)”(见 7.1.2.4);

——增加了“密码支持(FCS 类)”(见 7.1.3);

——增加了“用户数据保护(FDP 类)”中的“子集残余信息保护(FDP_RIP.1)”和“基本回退(FDP_ROL.1)”(见 7.1.4.9 和 7.1.4.10);

——增加了“安全管理(FMT 类)”中的“TSF 数据限值的管理(FMT_MTD.2)”(见 7.1.6.6);

——增加了“TSF 保护(FPT 类)”中的“失效即保持安全状态(FPT_FLS.1)”(见 7.1.7.1);

——增加了“资源利用(FRU 类)”(见 7.1.8);

——增加了 EAL3、EAL4 级的安全保障要求(见 7.2);

——修改了安全目的和安全要求的基本原理的规定(见 8.1 和 8.2);

——增加了组件依赖关系的规定(见 8.3)。

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:中国信息安全测评中心、兴唐通信科技有限公司、国网思极网安科技(北京)有限公司、北京元心科技有限公司、中国科学院软件研究所、北京邮电大学、中国信息通信研究院、展讯通信(上海)有限公司。

本标准主要起草人:张宝峰、贾炜、杨永生、石竑松、李凤娟、许源、殷树刚、宁华、饶华一、毕海英、

张骁、熊琦、邓辉、高金萍、张阳、梁洪亮、邹仕洪、毛军捷、王蓓蓓、庞博、朱瑞瑾、刘昱函、许勇刚、陈佳哲、李贺鑫、李祉岐、魏伟、孙亚飞、王宇航、王亚楠、李静、朱克雷、黄小莉、骆扬、王书毅、王峰、张翀斌、郭颖。

本标准所代替标准的历次版本发布情况为：

——GB/T 30284—2013。

信息安全技术　移动通信智能终端操作系统安全技术要求

1　范围

本标准规定了移动通信智能终端(以下简称移动终端)操作系统的安全功能要求和达到 EAL2、EAL3 和 EAL4 保障级的安全保障要求。

本标准适用于移动终端操作系统产品的设计、开发、测试和采购。

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 18336.1—2015　信息技术　安全技术　信息技术安全评估准则　第 1 部分:简介和一般模型

GB/T 18336.2—2015　信息技术　安全技术　信息技术安全评估准则　第 2 部分:安全功能组件

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

3　术语、定义和缩略语

3.1　术语和定义

GB/T 18336.1—2015 及 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1.1

管理员　administrator

一个授权用户,拥有管理部分或全部移动终端操作系统安全功能的权限,同时可拥有旁路部分移动终端操作系统安全策略的特权。

3.1.2

应用软件　application software

移动终端操作系统之外,向用户提供服务功能的软件。

3.1.3

鉴别数据　authentication data

用于验证用户所声称身份的信息。

3.1.4

授权用户　authorized user

依据安全策略可执行某项操作的用户。