



中华人民共和国认证认可行业标准

RB/T 182—2023

移动智能终端应用软件个人信息安全 评价规范

Evaluation specifications for personal information security of application software
in smart mobile terminals

2024-05-20 发布

2024-07-01 实施

国家认证认可监督管理委员会 发布
中国标准出版社 出版

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 评价流程	2
4.1 概述	2
4.2 评价主要环节	3
5 评价要求	4
5.1 组建团队	4
5.2 制定方案	4
5.3 实施评价	5
5.4 结果记录	5
6 评价内容及方法	5
6.1 个人信息的收集	5
6.2 个人信息的存储	10
6.3 个人信息的使用	13
6.4 个人信息主体的权利	17
6.5 个人信息的委托处理、共享、转让、公开披露	22
6.6 个人信息安全事件处置	31
6.7 组织的个人信息安全管理要求	32
7 评价结果判定	38
7.1 文档审核结果	38
7.2 技术验证结果判定	38
7.3 现场审核结果判定	38
7.4 认证决定	39
附录 A (规范性) 移动智能终端应用软件个人信息安全评价内容	40
附录 B (资料性) 评价项编码规则说明	45
参考文献	47

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。本文的发布机构不承担识别专利的责任。

本文件由国家认证认可监督管理委员会提出并归口。

本文件起草单位：中国网络安全审查认证和市场监管大数据中心、北京软件产品质量检测检验中心、上海市信息安全测评认证中心、中国电子科技集团公司第十五研究所、中国信息通信研究院、公安部第一研究所、北京邮电大学、中国科学院软件研究所。

本文件主要起草人：张晓梅、许静慧、辛建峰、王威、顾敏、胡石、袁翠红、陈淑娟、田晴云、何静、温岩莉、郝伟博、王艳红、任凤丽、韩煜、冀乃杰、苏璞睿、张淼、严妍、王也。

移动智能终端应用软件个人信息安全 评价规范

1 范围

本文件规定了移动智能终端应用软件个人信息安全的评价流程、评价要求、评价内容及方法和评价结果判定。

本文件适用于认证机构和技术验证机构对移动智能终端应用软件个人信息安全进行检测、评估和认证等活动。

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。

GB/T 35273—2020 信息安全技术 个人信息安全规范

3 术语和定义

GB/T 35273—2020 界定的以及下列术语和定义适用于本文件。

3.1

移动智能终端应用软件 application software in smart mobile terminal

针对移动智能终端开发的应用软件,包括移动智能终端预置的第三方应用软件,以及互联网服务提供者提供的通过网站、应用商店等移动应用分发平台下载、安装和升级的应用软件。

注:简称“App”。

[来源:GB/T 34975—2017,3.3,有修改]

3.2

认证机构 certification body

从事与产品、服务、过程、体系或人员有关的第三方证明活动的机构。

注:认证机构可以自己进行测试和检验活动,或者委托其他机构代表其进行这些活动。

[来源:RB/T 072—2021,4.6]

3.3

运营机构 operating organization

通过移动智能终端应用软件向用户提供信息服务的网络运营者,负责移动智能终端应用软件的运营,承担移动智能终端应用软件个人信息安全的法律责任。

3.4

技术验证 technical verification

专业技术人员采用测试、检查和文档核查等方法进行符合性验证的过程。