ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 43445—2023

信息安全技术　移动智能终端预置应用软件基本安全要求

Information security technology—Basic security requirements for pre-installed applications on smart mobile terminals

2023-11-27 发布　　2024-06-01 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。本文件的发布机构不承担识别专利的责任。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国电子技术标准化研究院、国家计算机网络应急技术处理协调中心、中国科学院信息工程研究所、中国科学院软件研究所、中国电子技术标准化研究院华东分院。

本文件主要起草人：郝春亮、周晨炜、张骁、姚相振、上官晓丽、胡影、王晖、卓子寒、刘玉岭、梁瑞刚、王姣、张严、周燕华。

信息安全技术　移动智能终端预置应用软件基本安全要求

1　范围

本文件规定了移动智能终端预置应用软件的基本安全要求。

本文件适用于移动智能终端的设计、开发、生产和测试，也适用于主管监管部门、第三方评估机构对移动智能终端进行监督、管理和评估。

本文件不适用于工业终端、车载终端等面向特定行业和用途的数据终端，也不适用于未接入公众移动通信网络的智能终端产品。

注：本文件中移动智能终端主要指以接入公众移动通信网络的智能手机为主的手持式移动智能终端产品。

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　信息安全技术　个人信息安全规范

GB/T 39720—2020　信息安全技术　移动智能终端安全技术要求及测试评价方法

GB/T 40660　信息安全技术　生物特征识别信息保护基本要求

3　术语和定义

下列术语和定义适用于本文件。

3.1

移动智能终端　smart mobile terminal

接入公众移动通信网络、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

预置应用软件　pre-installed application

由生产企业预置，在移动智能终端主屏幕和辅助屏界面内存在用户交互入口，为满足用户应用需求而提供的、可独立使用的软件程序。

3.3

基本功能软件　basic function application

直接支撑操作系统运行或实现移动智能终端基本功能所必需的预置应用软件。

4　安全功能要求

4.1　可卸载要求

4.1.1　移动智能终端中除基本功能软件之外的其他预置应用软件均应可卸载，基本功能软件应仅限于

以下范围：系统设置、文件管理、多媒体摄录、接打电话、收发短信、通讯录、浏览器、应用商店。

4.1.2 实现同一基本功能的预置应用软件，设置为不可卸载的不应超过一款。

4.1.3 基本功能软件内附带扩展功能软件（模块）时，应提供卸载或禁用扩展功能软件（模块）的方式。

4.2 卸载安全要求

预置应用软件的卸载安全要求包括：

a) 预置应用软件卸载后不应影响移动智能终端的正常使用，相关情形包括但不限于：造成系统安全环境破坏，导致系统崩溃等；

b) 可卸载预置应用软件应提供便捷的卸载功能；

注：例如在主屏幕通过长按应用软件图标提供便捷的应用软件卸载入口等。

c) 在不影响移动智能终端安全使用的情况下，附属于被卸载预置应用软件的资源文件、配置文件和用户数据等应能够被删除，同时应为用户提供保留用户数据、配置文件的卸载方式；

d) 移动智能终端操作系统升级时，已卸载的预置应用软件不应在未经用户授权的情况下被恢复，且升级后的预置应用软件应仍满足本文件要求。

4.3 安全技术要求

移动智能终端生产企业应确保预置应用软件符合 GB/T 39720—2020 中 6.3.1 b)、6.3.2、6.3.4 的要求。

4.4 个人信息安全要求

预置应用软件的个人信息安全要求包括以下内容。

a) 预置应用软件不应在用户未使用应用程序的具体功能时，提前获取相关权限或者收集个人信息。其中，基本功能软件可在移动智能终端开机向导中告知用户个人信息处理规则并征询同意；其他预置应用软件应仅在用户使用应用程序的具体功能时向用户申请该功能对应的必要权限和收集必要个人信息。

注：本文件中“权限”均指“可收集个人信息权限”，可收集个人信息权限范围见 GB/T 41391—2022 的附录 D。

b) 基本功能软件应在移动智能终端内处理敏感个人信息，确有必要传出移动智能终端的，应取得用户单独同意。用户选择不同意时，不应影响移动智能终端基本功能的正常使用。基本功能软件应在将敏感个人信息传出移动智能终端前，以显著方式明确告知用户。

c) 移动智能终端操作系统宜对预置应用软件提供与非预置应用软件相同的可收集个人信息权限的控制功能。

5 安全管理要求

5.1 预置环节安全管理

移动智能终端生产企业应采取技术措施预防在产品流通环节发生置换操作系统或安装应用程序的行为。

注：例如，防止系统版本回退、增加刷机复杂度、操作系统软件签名验签等。

5.2 预置应用软件安全管理

5.2.1 基本功能软件提供者安全能力要求

基本功能软件提供者（包括移动智能终端生产企业自身及第三方）的安全能力要求包括：

a） 涉及个人信息处理的，应符合 GB/T 35273 的要求；

b） 涉及个人生物识别信息处理的，应符合 GB/T 40660 的要求。

5.2.2 预置应用软件个人信息处理规范性审核验证

移动智能终端生产企业应在移动智能终端出厂前对预置应用软件进行个人信息处理活动规范性审核和测试验证。

5.3 预置应用软件安全信息明示

移动智能终端生产企业应通过产品说明书、官方网站、开机引导环节和用户首次使用预置应用软件前专门的个人信息处理规则，或设置移动智能终端内专门界面等至少一种渠道，对预置应用软件安全信息进行完整明示，包括但不限于：

a） 应用程序名称、功能描述；

b） 应用程序提供者名称；

c） 卸载方法；

d） 个人信息收集范围、使用目的；

e） 可收集个人信息权限申请范围；

f） 基本功能软件提供者的安全能力证明。

5.4 安全问题响应

移动智能终端生产企业应通过建立简单易用的投诉举报渠道等方式，确保能够响应用户反馈的预置应用软件安全问题。

参 考 文 献

[1] GB/T 41391—2022 信息安全技术 移动互联网应用程序(App)收集个人信息基本要求