ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术　智能手机预装应用程序基本安全要求

Information security technology — Basic security requirements for pre-installed applications on smartphones

（征求意见稿）

（本稿完成时间：2022 年 10 月 9 日）

XXXX－XX－XX 发布　　XXXX－XX－XX 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。

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、中国科学院软件研究所等。

本文件主要起草人：姚相振、郝春亮、周晨炜、上官晓丽、胡影、王晖、王姣、张严等。

信息安全技术　智能手机预装应用程序基本安全要求

1　范围

本文件给出了智能手机预装应用程序的基本安全要求。

本文件适用于智能手机生产企业的生产活动，也可为相关监管、第三方评估工作提供参考。

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 34975—2017　信息安全技术　移动智能终端应用软件安全技术要求和测试评价方法

GB/T 35273—2020　信息安全技术　个人信息安全规范

GB/T 37988—2019　信息安全技术　数据安全能力成熟度模型

GB/T 40660—2021　信息安全技术　生物特征识别信息保护基本要求

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

3　术语与定义

下列术语和定义适用于本文件。

3.1

智能手机　smartphone

能提供应用软件开发接口，并能安装和运行应用软件的具有通话功能的移动智能终端。

3.2

预装应用程序　pre-installed application

由智能手机生产企业自行或与移动互联网应用程序运营者合作在智能手机出厂前安装的，在智能手机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、可独立使用的应用程序。

3.3

第三方预装应用程序　third-party pre-installed application

由智能手机生产企业之外的其他法人实体提供的预装应用程序。

4　安全技术要求

4.1　可卸载要求

4.1.1 可卸载范围

4.1.1.1 除系统设置、文件管理、多媒体摄录、接打电话、收发短信、通讯录、浏览器、应用商店等直接支撑操作系统运行或实现智能手机基本功能所必须的基本功能应用程序外，智能手机中其他预装应用程序均应可卸载。

4.1.1.2 实现同一基本功能的预装应用程序，至多有一款可设置为不可卸载。

4.1.2 不可卸载预装应用程序要求

不可卸载应用程序内含有直接支撑操作系统运行或实现智能手机基本功能之外的其他功能时，应提供禁用或卸载这些功能的方式。

4.1.3 卸载安全要求

对预装应用程序的卸载安全要求包括：

a) 预装应用程序卸载后不应影响智能手机的正常使用，包括但不限于：不应造成系统安全环境破坏，不应导致系统崩溃等；
b) 可卸载预装应用程序应提供便捷的卸载功能，例如通过长按桌面图标方式卸载等；
c) 在不影响智能手机安全使用的情况下，卸载预装应用程序应将相关程序文件及数据完全删除，用户选择保留的用户数据、配置文件除外；
d) 应确保已被卸载的预装应用程序在智能手机操作系统升级时不被恢复，同时应保证升级后的预装应用程序仍满足本文件 4.1.1 要求。

4.2 安全功能及保障要求

预装应用程序的安全功能及安全保障应符合 GB/T 34975—2017 要求。

4.3 个人信息安全要求

对预装应用程序的要求包括：

a) 预装应用程序收集个人信息应符合 GB/T 41391—2022 要求；
b) 预装应用程序应仅在用户开始对该应用程序进行交互操作后向用户申请相关系统以及个人信息权限，不应在用户未进行交互操作前获取相关权限；
c) 不可卸载应用程序宜提供停止使用功能，用户选择停止使用后，不可卸载应用程序不应再对用户个人信息进行处理；
d) 预装应用程序将敏感个人信息传出智能手机的，应取得用户单独同意。智能手机生产企业应确保用户选择不同意时不影响智能手机基本功能的使用，并在征求同意时将该情况明确告知用户。

5 安全管理要求

5.1 预装行为安全

智能手机生产企业应采取技术和管理措施预防在产品流通环节发生置换操作系统和安装应用程序的行为，确保智能手机获得进网许可证前后预装应用程序的范围和可卸载性保持一致。

5.2 第三方预装应用程序安全管理

5.2.1 第三方安全能力审核

智能手机生产企业应对第三方预装应用程序提供者的数据安全和个人信息保护能力进行审核，对第三方预装应用程序提供者的安全能力要求包括：

a) 数据安全能力宜至少符合 GB/T 37988—2019 二级能力要求，或通过数据安全能力相关认证；
b) 涉及个人信息处理的，应符合 GB/T 35273—2020 要求；
c) 涉及个人生物识别信息处理的，应符合 GB/T 40660—2021 要求。

5.2.2 第三方预装应用程序个人信息安全审核

智能手机生产企业应在预装第三方应用程序前，对第三方预装应用程序的个人信息处理规则进行审核，包括但不限于审核以下内容的真实性和合理性：

a) 应用程序基本信息，包括应用程序名称、包名、版本号、更新日期、安装文件；
b) 应用程序提供者信息，包括应用程序提供者名称、联系方式；
c) 个人信息保护政策，包括生效日期、全文文本、可查看全文的有效链接；
d) 收集的个人信息范围，包括提供的服务类型、收集的个人信息类型以及通过收集的个人信息所实现的业务功能或使用目的；
e) 申请的可收集个人信息权限列表，包括权限名称、相关业务功能/使用目的、用户能否拒绝授权；
f) 涉及到收集个人信息的第三方 SDK 信息，包括名称、包名、提供者名称、嵌入目的、SDK 收集的个人信息类型、SDK 使用的可收集个人信息权限；
g) 第三方预装应用程序提供者关于收集个人信息的工具或手段的声明。

5.3 预装应用程序安全信息公示

智能手机生产企业应在产品说明书、官方网站，以及智能手机首次使用时，对预装应用程序安全信息进行明示，包括：

a) 应用程序名称、版本号；
b) 应用程序提供者名称、联系方式；
c) 是否可卸载、卸载方法；
d) 个人信息收集范围及使用目的；
e) 可收集个人信息权限申请范围及使用目的；
f) 第三方预装应用程序的安全测试、认证情况；
g) 其他安全信息。

5.4 投诉举报

智能手机生产企业应建立简单易用的投诉举报渠道，并确保用户反馈的预装应用程序安全问题能够及时有效处理。

参 考 文 献

[1] 工业和信息化部关于印发《移动智能终端应用软件预置和分发管理暂行规定》的通知（2016 年 12 月 23 日工业和信息化部发布）

[2] 公开征求对《关于进一步规范移动智能终端应用软件预置行为的通告》的意见（2022 年 2 月 16 日工业和信息化部信息通信管理局发布）

[3] 国家互联网信息办公室关于《网络数据安全管理条例（征求意见稿）》公开征求意见的通知（2021 年 11 月 14 日国家互联网信息办公室发布）

[4] App 违法违规收集使用个人信息行为认定方法（2019 年 12 月 30 日国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局发布）