ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 43435—2023

信息安全技术　移动互联网应用程序(App)软件开发工具包(SDK)安全要求

Information security technology—Security requirements for software development kit (SDK) in mobile internet applications (App)

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：每日互动股份有限公司、中国电子技术标准化研究院、中国网络安全审查技术与认证中心、中国信息通信研究院、北京百度网讯科技有限公司、安徽工程大学、蚂蚁科技集团股份有限公司、华为技术有限公司、公安部第一研究所、国家计算机病毒应急处理中心、高德软件有限公司、北京快手科技有限公司、罗克佳华科技集团股份有限公司、荣耀终端有限公司、友盟同欣(北京)科技有限公司、公安部第三研究所、国家信息技术安全研究中心、国家计算机网络应急技术处理协调中心、浙江省大数据联合计算中心有限公司、北京奇虎科技有限公司、北京小桔科技有限公司、小米通讯科技有限公司、OPPO广东移动通信有限公司、阿里巴巴(北京)软件服务有限公司、北京抖音信息服务有限公司、秒针信息技术有限公司、上海兆言网络科技有限公司、杭州云深科技有限公司、浙江大学、复旦大学、神策网络科技(北京)有限公司、启明星辰信息技术集团股份有限公司、北京智游网安科技有限公司、上海合合信息科技股份有限公司、华住酒店管理有限公司、上海游昆信息技术有限公司、科大讯飞股份有限公司、同盾科技有限公司、贝壳找房(北京)科技有限公司、深圳海云安网络安全技术有限公司、北京指掌易科技有限公司、北京腾云天下科技有限公司、泰尔卓信科技(北京)有限公司。

本文件主要起草人：董霖、方毅、刘行、周程、胡影、金岩、郄世杰、樊华、田晴云、何延哲、李浩川、武林娜、常浩伦、李颖莹、韩淼淼、彭婕、邓婷、徐雨晴、安泽亮、白晓媛、衣强、韩煜、刘彦、张鑫、黄玥澎、王昕、郭变香、赵晓娜、贾紫薇、田宇轩、张艳、曹岳、林星辰、王一宇、易立、姚一楠、张娜、黄香敏、付艳艳、黄天宁、田申、李昳婧、高雅、严涵、吕繁荣、尹祖勇、王秋、解伯延、汤立波、臧磊、周亚金、郑磊、李腾、魏超、张昀、王彬、沈林、余明明、史景、桑文锋、姚栋、谭成、李彪、谢朝海、落红卫、蔡欣奕、刘笑岑、张朝、葛梦莹、刘桢。

信息安全技术　移动互联网应用程序(App)软件开发工具包(SDK)安全要求

1　范围

本文件规定了移动互联网应用程序(App)软件开发工具包(SDK)设计、开发、发布、运营、终止运营等阶段和个人信息处理活动的安全要求。

本文件适用于SDK开发、运营,并供SDK安全检测和评估参考使用。

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 25069—2022　信息安全技术　术语

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 37964—2019　信息安全技术　个人信息去标识化指南

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　术语和定义

GB/T 25069—2022、GB/T 35273—2020、GB/T 41391—2022界定的以及下列术语和定义适用于本文件。

3.1

软件开发工具包　software development kit;SDK

协助软件开发的软件库。

注:软件开发工具包通常包括相关二进制文件、API、文档、范例和工具的集合。

[来源:GB/T 41391—2022,3.14,有修改]

3.2

软件开发工具包运营者　software development kit operator

软件开发工具包的开发者、所有者、管理者或提供者。

注:简称SDK运营者,也包括SDK相关的个人信息处理者。

3.3

移动互联网应用程序运营者　mobile internet application operator

移动互联网应用程序的开发者、所有者、管理者或提供者。

注:简称App运营者,也包括App相关的个人信息处理者。

[来源:GB/T 41391—2022,3.2,有修改]

3.4

最终用户　end user

在移动终端设备上使用移动互联网应用程序的用户。

3.5

热更新　hot update

通过动态下发和加载代码，在 App 或 SDK 不重新下载和安装的情况下，改变其原有代码逻辑或资源文件。

3.6

公共仓库　public repository

方便开发者上传和下载源码或者二进制程序的公共平台。

4　概述

4.1　SDK 使用场景

SDK 运营者将实现特定功能的代码开发并封装成 SDK，App 运营者将 SDK 嵌入其开发的 App 中，最终用户通过 App 使用 SDK 提供的功能，例如广告、推送等，常见 SDK 服务类型见附录 A。

4.2　SDK 安全风险

最终用户在 SDK 使用过程中存在的安全风险主要包括：

a）　SDK 安全漏洞，由于 SDK 技术方案不合理或者因自身代码缺陷产生的技术层面的安全隐患和风险，例如弱加密算法漏洞等，常见 SDK 安全漏洞见附录 B；

b）　SDK 恶意行为，利用 SDK 进行违法、非正当的行为，例如广告刷量等，常见 SDK 恶意行为见附录 C；

c）　SDK 处理个人信息安全问题，SDK 运营过程中涉及个人信息处理的安全问题，例如超范围收集个人信息等，常见 SDK 处理个人信息安全问题见附录 D。

5　SDK 设计、开发、发布、运营、终止运营等阶段安全要求

5.1　设计

SDK 设计阶段的安全要求包括：

a）　SDK 应仅包含与其声明功能相符合的功能，功能设计应符合正当、必要的原则；

b）　SDK 宜提供单独控制热更新功能开启或关闭的选项，并确保 App 运营者在不接受热更新功能的情况下仍可正常使用 SDK 其他功能；

c）　在非服务所必需或者无合理场景下，SDK 不应自启动或者关联启动其他 App。

5.2　开发

SDK 开发阶段的安全要求包括：

a）　应满足 GB/T 34975—2017 中 4.1.5.1、4.1.5.2、4.1.5.3 的要求；

b）　SDK 运营者应对 SDK 进行安全自评估，如代码审计、安全漏洞扫描、隐私合规检测等；

c）　SDK 运营者宜对广告、支付、认证、安全风控等安全要求较高的 SDK 进行第三方安全测评；

d）　SDK 运营者应对 SDK 中集成使用的第三方代码和/或组件进行安全检测。

5.3 发布

SDK 发布阶段的安全要求包括：

a) SDK 运营者应通过官方网站、开源社区、公共仓库或以其他方式提供 SDK 下载文件、集成文档和 API 文档、隐私政策、问题反馈和投诉渠道等信息；

b) SDK 运营者应在官方网站、开源社区或集成文档中提供隐私政策，并在隐私政策中声明 SDK 所具有的全部功能和个人信息处理规则，告知的信息应完整、准确、及时，不存在故意隐瞒、欺骗等行为；

c) SDK 运营者发布 SDK 时应提供相关的数字签名（包括 SDK 运营者和/或第三方安全测评机构签发的数字签名）；

d) 通过公共仓库进行 SDK 发布时，SDK 运营者应对公共仓库账号进行妥善保管，避免因公共仓库账号泄露引发的安全风险。

5.4 运营

SDK 运营阶段的安全要求包括：

a) SDK 运营者应向 App 运营者提供 SDK 安全能力说明及安全评估报告（包括自评估和/或第三方安全测评机构报告），如数据安全存储、数据安全交互、关键组件安全配置、代码及资源文件安全等方面；

b) 如 SDK 存在热更新机制，SDK 运营者应在热更新推送前向 App 运营者告知本次热更新的具体内容及可能造成的影响，在涉及用户利益受损的紧急情况下，SDK 运营者应当在紧急情况消除后及时告知；如热更新内容涉及个人信息处理目的、方式和范围的变更，应通过邮件、电话等逐一送达方式告知 App 运营者，并宜通过 App 征得用户同意后再推送更新；

c) SDK 运营者如在运营期间发现 SDK 安全漏洞，应告知 App 运营者，并按照有关规定完成漏洞处置以及配合 App 运营者重新集成修复后的 SDK；

d) 如 App 运营者与 SDK 运营者分属不同的法人实体，SDK 运营者应与 App 运营者通过合同等形式明确双方的安全责任及应实施的个人信息安全措施，约定 App 运营者应当通过隐私政策等文件将 SDK 在 App 中实际处理个人信息的目的、方式、处理的个人信息种类、保存期限、个人信息主体行使权利的方式等规则告知最终用户；

e) SDK 运营者如发现 App 运营者未能向最终用户告知 SDK 个人信息处理规则，或授权同意方式不符合要求的，应主动提示其及时改进；如果 App 运营者在约定时间内未完成改进的，SDK 运营者应当停止向其继续提供服务；

f) SDK 运营者应建立响应个人信息主体请求和投诉机制，个人信息主体可通过 App 运营者向 SDK 运营者进行请求和投诉；

g) 因 SDK 引发个人信息安全事件的，SDK 运营者应按照 GB/T 35273—2020 的第 10 章关于个人信息安全事件处置的要求进行处置；

h) SDK 运营者应按照 GB/T 35273—2020 的第 11 章落实组织的个人信息安全管理要求。

5.5 终止运营

SDK 终止运营阶段的安全要求包括：

a) SDK 运营者在终止运营前，应提前告知受影响的 App 运营者；

b) SDK 运营者在终止运营后，应按照 6.7c)的要求对个人信息进行处理。

6 SDK 个人信息处理安全要求

6.1 个人信息收集

SDK 个人信息收集的安全要求包括以下内容。

a) 应满足 GB/T 35273—2020 中第 5 章的要求。

b) SDK 运营者应明确个人信息处理规则和保护责任，包括：

1) SDK 收集的个人信息的目的、方式、范围；
2) SDK 申请的系统权限和申请目的；
3) SDK 收集的个人信息的保存期限、被停止嵌入后的个人信息处理方式；
4) 个人信息安全责任和保护措施；
5) SDK 是否存在热更新机制；
6) SDK 是否存在自启动、关联启动；
7) SDK 收集的个人信息是否涉及向境外提供；
8) SDK 自行或协助 App 响应用户个人信息权利请求的措施。

c) SDK 收集的个人信息不应超出隐私政策等方式中声明的个人信息收集范围。

d) SDK 在保证功能正常前提下应以最小范围收集个人信息。

注：范围通常涉及收集个人信息的类型、频率、数量、精度等。

e) SDK 应仅声明和申请实现 SDK 服务目的最小范围的系统权限，不应申请与 SDK 功能无关的系统权限。

f) 在最终用户或 App 运营者未使用 SDK 提供的某项业务功能时，SDK 不应主动通过 App 申请或使用 App 已申请的该项业务功能所需的权限。

g) SDK 收集个人信息前，应通过 App 征得最终用户同意。

h) SDK 收集敏感个人信息前，应通过 App 征得最终用户单独同意。

6.2 个人信息存储

SDK 个人信息存储的安全要求包括：

a) 应满足 GB/T 35273—2020 中 6.1 的要求；

b) SDK 运营者应对 SDK 运行所使用的文件、数据库中的敏感个人信息进行加密存储以及完整性校验，避免个人信息泄露或被篡改。

6.3 个人信息使用和加工

SDK 个人信息使用和加工的安全要求包括：

a) 应满足 GB/T 35273—2020 中第 7 章的要求；

b) SDK 运营者对个人信息的使用和加工方式应与隐私政策等形式中声明的内容保持一致，如汇聚融合、用户画像等；

c) SDK 运营者如果需要对收集个人信息的使用或加工的目的进行变更，应重新告知 App 运营者，并通过 App 告知用户并征得用户同意；

d) SDK 运营者人员访问通过 SDK 收集的个人信息，应进行访问控制，并遵循最小必要授权原则；

e) SDK 应优先在移动终端本地使用和加工个人信息。

6.4 个人信息传输

SDK 个人信息传输的安全要求包括：

a） SDK 传输敏感个人信息前应提供区别其他个人信息的安全保障，如采取合适的方式对敏感个人信息进行单独加密；

b） SDK 运营者与 App 运营者之间传输敏感个人信息应采取加密处理等技术安全措施。

6.5 个人信息提供

SDK 个人信息提供的安全要求包括：

a） 应满足 GB/T 35273—2020 中 9.1、9.2、9.6 的要求；

b） SDK 运营者向 App 运营者之外的其他机构或个人提供其处理的个人信息，应按照法律法规规定取得直接或间接用户授权，在间接用户授权的情况下，SDK 运营者应当对用户授权情况进行核查、并留存核查记录；

注：直接用户授权指最终用户授权 SDK 运营者向 App 运营者之外的其他机构或个人提供其个人信息；间接用户授权指最终用户授权 App 运营者之外的其他机构或个人从 SDK 运营者共享个人信息。

c） SDK 运营者向 App 运营者之外的其他机构或个人提供其处理的个人信息时，宜进行匿名化或去标识化处理，去标识化处理的过程可依据 GB/T 37964—2019 的第 5 章；

d） SDK 运营者向 App 运营者之外的其他机构或个人提供个人信息时，应与数据接收方通过合同等形式明确双方的责任和义务。

6.6 个人信息公开

SDK 运营者不应公开其处理的个人信息。

6.7 个人信息删除

SDK 个人信息删除的安全要求包括：

a） SDK 运营者应向 App 运营者提供个人信息删除机制，最终用户可通过 App 行使个人信息删除权利，SDK 运营者应在接收到 App 运营者关于最终用户的个人信息删除的请求后，在服务器端删除其收集的个人信息或做匿名化处理；

b） App 运营者停止接入 SDK 并通知 SDK 运营者后，SDK 运营者应停止继续通过该 App 收集个人信息，若 SDK 运营者存在收集个人信息的，应按照双方合作协议中约定的个人信息处理要求和最终用户的授权范围，在服务器端删除其收集的个人信息或做匿名化处理；

c） SDK 停止运营后，应在服务器端删除其收集的个人信息或做匿名化处理。

附 录 A
（资料性）
常见 SDK 服务类型

表 A.1 列出了常见 SDK 服务类型。

表 A.1 常见 SDK 服务类型

服务类型	基本功能	典型子类别	功能描述
广告类	提供广告展示(在特定广告位上展示由广告主投放的广告信息的功能)、监测归因等功能	广告投放	通过插屏广告、浮层广告、原生广告、激励广告等形式向用户展示广告
		广告监测	帮助广告主了解广告投放的状况、广告投放策略的分析、广告的效果评估，并提供广告投放的结算依据
推送类	提供应用相关的通知或消息推送功能	无	提供应用相关的通知或消息推送功能
地图类	提供地图展示、位置定位、路径导航功能	地图展示	用于显示地图内容，包含二维、三维地图等数据
		定位	提供精确或粗略定位能力
		导航	提供路径规划的能力，并能根据路况、交通工具和偏好提供多种规划方案
支付类	提供移动支付、收单功能等金融业务且保障用户的账户、资金等金融业务安全	无	提供移动支付、收单功能等金融业务且保障用户的账户、资金等金融业务安全
框架类	提供开发某一类 App 或跨平台 App 所需的整体框架	UI 框架类	提供用户界面(UI)解决方案
		网络框架类	简化网络访问功能的开发
		存储框架类	优化存储访问速度，简化开发过程
		文件下载类	提供内容分发网络(CDN)、对象存储等数据下载的服务
		架构框架类	提供整体的架构方案，优化项目结构和流程
		多媒体框架类	提供音视频编解码、PDF 渲染、音视频编辑、图片编辑等能力
		游戏引擎类	2D/3D/物理引擎
		浏览器框架类	提供内嵌浏览器
		跨平台开发框架	提供跨各类移动操作系统以及 Web 等平台的应用开发框架，以及小程序/小游戏框架

表 A.1　常见 SDK 服务类型（续）

服务类型	基本功能	典型子类别	功能描述
统计类	通过埋点等方式，通过数据化图表等多种形式进行数据统计分析	统计分析	提供统计分析服务。帮助 App 开发者分析用户行为、属性等，更新完善产品，提高用户体验
		测试	提供线上测试功能，如 A/B 测试
性能监控类	提供 App 崩溃、App 无响应、卡顿等异常数据的收集与分析	无	提供 App 崩溃、App 无响应、卡顿等异常数据的收集与分析
登录类	提供手机号、账号登录功能	手机号登录	提供基于移动运营商的一键登录服务和基于短信验证的登录服务
		第三方账号登录	提供通过其他第三方账号体系登录 App 的功能
认证类	提供生物特征识别、身份认证等功能	生物特征认证类	提供人脸、声纹等生物特征认证功能
		身份认证	提供身份证识别、实名认证功能
		短信验证类	提供短信验证功能
社交类	提供社交功能，如消息、分享、排行等功能	即时通信类	提供即时通信能力，包括基于文字、图像、语音的点对点聊天、群聊天等
		社交分享类	帮助开发者实现社会化分享、登录、关注、获取好友列表等社会化功能
实时音视频类	提供实时音视频相关服务功能	音视频通话类	提供实时音视频通话相关功能
		直播类	针对直播场景提供直播推流/拉流、互动等服务，满足移动直播和互动需求
客服类	提供客服对话窗口、客服机器人等客服功能，实现用户与客服便捷沟通、问题跟踪以及客服动态分配等功能	无	提供客服对话窗口、客服机器人等客服功能，实现用户与客服便捷沟通、问题跟踪以及客服动态分配等功能
安全风控类	提供移动业务安全风控功能	加固类	通过技术手段对应用进行加固，防止应用被逆向、篡改、调试等，保护应用的安全
		风控类	通过技术手段防止应用被恶意篡改、恶意刷量，防作弊，从而保护开发者
		加密类	提供密钥管理服务和常用加解密算法功能
		VPN 类	提供虚拟专用网络（VPN）拨号连接服务

表 A.1　常见 SDK 服务类型（续）

服务类型	基本功能	典型子类别	功能描述
人工智能类	基于人工智能技术，提供音频、视频、图片、文本的计算服务	图像识别	提供基于人工智能的图像识别服务
		语音合成	提供基于人工智能的语音合成服务
		语音识别	提供基于人工智能的语音识别服务
		文本识别	提供基于人工智能的文本识别服务
		AR/VR/MR	提供增强现实（AR）/虚拟现实（VR）/混合现实（MR）服务
		图像增强	提供基于人工智能的图像优化处理服务，如美颜、超分辨率、风格化等
平台服务类	输出平台的能力，功能主要依托平台能力实现	电商服务	提供电商服务内容
		内容服务	输出平台内容，如微博、音乐、视频等

附 录 B
（资料性）
常见 SDK 安全漏洞

表 B.1 列出了常见 SDK 安全漏洞。

表 B.1 常见 SDK 安全漏洞

类型	名称
源文件安全	Java 代码未混淆风险
	私有函数调用风险
	弱加密算法漏洞
	随机数不安全使用风险
	敏感函数调用风险
内部数据交互安全	低保护级别的自定义权限
	PengdingIntent 不安全使用
	携带敏感信息的隐式 Intent 调用
	动态注册广播风险
	FFmpeg 任意文件读取漏洞
	Intent Scheme URLs 攻击
	Provider 文件目录遍历漏洞
	Fragment 注入漏洞
	Webview 未移除隐藏接口
	Webview 明文保存密码
	Activity 绑定 browserable 与自定义协议
	剪切板读写操作漏洞
通信数据传输安全	安全套接层(SSL)通信客户端检测信任任意证书
	超文本传输安全协议(HTTPS)关闭主机名验证
	中间人攻击漏洞
	Webview 存在本地 Java 接口
	Webview 忽略 SSL 证书错误
	开放 socket 端口漏洞
	Webview 启用访问文件数据
本地数据存储安全	getdir 读写权限配置错误
	全局文件读写权限配置错误
	配置文件读写权限配置错误
	硬编码密钥漏洞
	打开或创建数据库文件权限配置错误

表 B.1　常见 SDK 安全漏洞（续）

类型	名称
防御检测	Dex 文件动态加载风险
	外部加载 so 文件漏洞
	未使用编译器堆栈保护技术
	未使用地址空间随机化技术
	unzip 解压缩漏洞
	动态链接库中包含执行命令函数
	libupnp 栈溢出漏洞
	Webview 组件远程代码执行（调用 getClassLoader）
	保存明文数字证书风险
	篡改/二次打包风险
	资源文件泄露风险
	so 文件破解风险
运行时异常	索引越界异常
	空指针异常
	非法参数异常
	类无法加载异常
	输入输出异常
	文件不存在异常

附 录 C
（资料性）
常见 SDK 恶意行为

表 C.1 列出了常见 SDK 恶意行为。

表 C.1 常见 SDK 恶意行为

序号	行为名称	注释
1	流量劫持	SDK 信息拉取、上报和展示目标与 App 运营者设定的目标不同，恶意劫持 App 流量，对 App 运营者造成损害
2	资费消耗	SDK 通过消耗最终用户网络套餐资费、恶意发送收费短信、订阅收费服务等行为，造成最终用户的资金损失
3	静默下载安装	SDK 在后台静默下载、安装其他恶意软件或病毒木马
4	广告刷量	SDK 在最终用户不知情的情况下，在后台模拟人工点击广告链接进行牟利
5	恶意广告	SDK 向最终用户推送包含欺诈内容、病毒木马的广告链接。推送过量广告，长期占用系统通知栏、屏幕界面，干扰最终用户正常使用 App
6	恶意勒索	SDK 恶意加密最终用户手机中的文件，干扰最终用户对手机的正常使用，并以恢复正常使用为由向最终用户勒索钱财
7	虚拟币挖矿	SDK 在最终用户不知情的情况下利用其手机的计算能力来为攻击者获取电子加密货币，对最终用户设备硬件造成性能损耗
8	远程控制	SDK 在移动终端启动本地后台服务端，接收远程控制端发来的控制指令，隐蔽进行其他恶意行为
9	剪切板劫持	SDK 对系统剪切板进行监听，根据剪贴板内容的变化触发悬浮窗，干扰系统功能，欺骗最终用户，或者影响其他应用正常使用

附 录 D
（资料性）
常见 SDK 处理个人信息安全问题

表 D.1 列出了常见 SDK 处理个人信息安全问题。

表 D.1 常见 SDK 处理个人信息安全问题

序号	个人信息处理活动	行为名称	注释
1	收集	SDK 超范围收集个人信息	SDK 收集与提供服务无关的个人信息，强制申请非必要的权限，自动收集个人信息的频度和时机不合理等
2		用户无法明确获知 SDK 收集使用个人信息的目的、类型、方式等	由于 SDK 未向 App 告知或未完整告知自身收集使用个人信息的规则，或者 SDK 向 App 完整告知了收集使用个人信息的规则但 App 未向最终用户说明等原因，造成最终用户对 SDK 收集使用个人信息的行为无感知
3		SDK 未经最终用户同意收集使用或对外提供个人信息	SDK 未经最终用户同意，私自调用系统权限隐蔽收集个人信息，私自通过自启动、关联启动等方式收集个人信息，实际调用的系统权限和收集的个人信息超出公开文档所声明的系统权限和个人信息
4		欺骗诱导用户提供个人信息	非服务所必需或无合理场景，通过积分、奖励、优惠等方式欺骗误导用户向 SDK 提供个人信息
5	存储	SDK 不安全存储个人信息	SDK 采用不安全的方式在移动终端存储个人信息，可能导致个人信息被 App 运营者和 SDK 运营者之外第三方获取
6	使用和加工	违规使用个人信息	SDK 超出其声明的收集使用个人信息的规则，将个人信息使用和加工用于其他目的
7	传输	SDK 不安全传输个人信息	SDK 使用不安全的网络协议传输个人信息，存在被拦截或者恶意篡改的风险
8	提供	违规对外提供个人信息	SDK 运营者未经最终用户同意将个人信息提供给 App 运营者和 SDK 运营者之外第三方
9	删除	未按要求删除个人信息	SDK 运营者在 App 运营者停止接入 SDK 或在 SDK 停止运营后，未及时对个人信息进行删除，存在个人信息泄露风险