电 信 终 端 产 业 协 会 标 准

TAF-WG4-AS0057-V1.0.0:2020

移动智能终端应用软件 SDK 安全技术要求

Security Technical Requirements of Software Development Kit for Applications on Smart Mobile Terminal

2020-04-09 发布　　2020- 04-09 实施

电 信 终 端 产 业 协 会　发 布

目　　次

前　　言

本标准按照 GB/T 1.1-2009给出的规则编写。

本标准由电信终端产业协会提出并归口。

本标准起草单位：中国信息通信研究院、维沃移动通信有限公司、阿里巴巴(中国)有限公司、北京三星通信技术研究有限公司

本标准主要起草人： 王宇晓、周飞、王江胜、王艳红、武林娜、杜云、陈鑫爱、焦四辈、宁华、白晓媛、吴春雨

移动智能终端应用软件 SDK 安全技术要求

1 范围

本标准规定了移动智能终端应用软件SDK的安全技术要求。

本标准适用于在移动智能终端应用软件上集成使用的SDK，移动智能终端应用软件包括预置应用软件以及通过其他途径安装的可集成使用SDK的应用软件。

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，仅所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 25069 信息安全技术 术语

YD/T 2407 移动智能终端安全能力技术要求

YD/T 3228 移动应用软件安全评估方法

GB/T 34978 信息安全技术 移动智能终端个人信息保护技术要求

YD/T 3082 移动智能终端上的个人信息保护技术要求

3 术语、定义和缩略语

3.1 术语和定义

GB/T 25069中界定的以及下列术语和定义适用于本文件。

3.1.1

移动智能终端 Smart Mobile Terminal

移动智能终端是指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。

3.1.2

移动智能终端操作系统 Operator System of Smart Mobile Terminal

移动智能终端最基本的系统软件，它控制和管理移动智能终端各种硬件和软件资源，并提供应用程序开发接口。

3.1.3

移动智能终端应用软件 Mobile Application

移动智能终端应用软件（以下简称“应用软件”）是指移动智能终端预置以及通过网站、应用商店、扫二维码、应用自身、其他线上线下平台或渠道下载、安装、升级、卸载的应用软件。

3.1.4

移动智能终端应用软件分发服务 Mobile Application Distribution Service

移动智能终端应用软件分发服务是指为用户提供应用软件下载、安装、升级、卸载及其他辅助应用软件分发相关的服务。

--包括移动应用商店、社交软件、浏览器等提供应用软件下载、安装、升级、卸载及其他辅助应用软件分发相关的服务。

3.1.5

移动智能终端预置应用软件 Pre-installed Application of Smart Terminal

移动智能终端预置应用软件是指由生产企业自行或与互联网信息服务提供者合作在移动智能终端出厂前安装的应用软件，以及终端生产企业官方在线系统升级时新增加的应用软件。

3.1.6

互联网信息服务提供者 InternetServiceProvider

互联网信息服务提供者是指提供互联网服务的公司

3.1.7

软件开发工具包 SDK

软件开发工具包为特定的软件包、软件框架、硬件平台、操作系统等创建应用软件的开发工具的集合

3.1.8

应用编程接口 API

预先定义的函数，提供应用程序与开发人员基于某软件或硬件得以访问一组例程的能力

3.1.9

危险权限 Dangerous Permission

危险权限是指Google定义需用户同意的运行时权限，涵盖应用需要涉及用户隐私信息的数据或资源，或者可能对用户存储的数据或其他应用的操作产生影响的区域

3.1.10

闭源 Closed Source

闭源指被用于任何没有资格作为开源许可术语的程序。一般的情况下，将仅能获得它们许可的计算机程序的一个二进制版本，而没有这个程序的源代码。

3.1.11

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或 者反映特定自然人活动情况的各种信息。

注 1:个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系 方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生 理信息、交易信息等。

注 2:个人信息控制者通过个人信息或其他信息加工处理后形成的信息，例如用户画像或特征标

签，能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的， 属于个人信息。

3.1.12

个人敏感信息 personal sensitive information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健 康受到损害或歧视性待遇等的个人信息。

注 1:个人敏感信息包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产 信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下(含)儿童 的个人信息等。

注 2:个人信息控制者通过个人信息或其他信息加工处理后形成的信息，如一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等 的，属于个人敏感信息。

3.1.3

Root （Android）

它使得用户可以获取Android操作系统的超级用户权限。Root能够帮助用户越过手机制造商的限制，运行需要系统权限的动作。Android系统的Root与苹果iOS系统的越狱类似。

3.2 缩略语

下列缩略语适用于本文件。

SDK	Software Development Kit	软件开发工具包
APP	Application	移动应用软件
HTTPS	HyperText Transfer Protocol Secure	超文本传输安全协议

4 移动智能终端应用软件 SDK 简介

4.1 移动智能终端应用软件 SDK 基本情况

SDK是Software Development Kit的缩写，中文名称为软件开发工具包。开发者在软件开发过程中，可能引入第三方服务公司开发的以代码或运行库的方式的工具包（本文以下简称为SDK）。SDK通常可以区分为系统SDK和应用SDK.系统SDK主要是为特定的软件包,软件框架,硬件平台,操作系统等应用时所使用的开发工具集合。应用SDK是基于系统SDK开发的独立于具体业务而具有特定功能的集合。本标准中目前所要求的范围主要为应用SDK。

SDK作为第三方服务公司通过代码或运行库的方式,为应用开发者提供某些具体功能,如图片预览、广告、推送消息、地图服务、数据服务等。SDK可提供广泛的功能，部分SDK只完成本地功能，并不进行网络连接和网络数据处理，其风险相对较小，集成和运行机制较为简单。具备网络连接功能和通过网络进行数据处理的SDK，其集成和运行机制较为复杂，其中包括SDK与远程服务器直接通信的方式和内置服务器启动后通信等多种方式。

SDK作为应用软件中重要组成部分，可同应用软件使用同样的系统环境，读取移动智能终端上的个人信息，存在着SDK滥用功能权限、过度收集使用个人信息、应用软件无法实际控制SDK、SDK与应用软件角色责任复杂等现状问题。

4.2 移动智能终端应用软件与 SDK 角色关系

移动智能终端应用软件与SDK角色关系介绍

角色	描述	责任	提供信息
SDK开发者	生产SDK，负责实现隐私保护和安全编码开发.	安全开发	使用的权限列表，收集使用的个人信息。
SDK运营者	运营SDK，提供运营服务，提供服务器，管理后台数据及进行隐私保护等。	安全运营	安全运营相关信息
应用软件提供者	开发应用软件，集成第三方SDK，依据合理性、必要性、辅助性、最小化评估并选择第三方SDK。	安全开发	集成的第三方 SDK 列表，及其所需权限、收集使用的个人信息
应用软件运营者	运营应用软件，提供运营服务，提供服务器，管理后台数据及隐私保护等	安全运营	安全运营相关信息

角色	SDK开发者	SDK运营者	应用软件提供者	应用软件运营者
SDK开发者	--	--	--	--
SDK运营者	代码使用权协议	--	--	--
应用软件提供者	代码使用权协议	--	--	--
应用软件运营者	--	服务协议	代码使用	--

移动智能终端应用软件提供者和运营者统称为移动应用软件提供方，SDK开发者和运营者统称为SDK提供方。

5 移动智能终端应用软件 SDK 安全技术要求

5.1 安全集成要求

（1） 应用软件所集成使用的SDK为闭源SDK，SDK提供方应保证其安全性，应用软件提供方集成SDK时应保证其所集成的为安全SDK。

（2） SDK提供方应主动提供相关信息，供应用软件提供者和运营者做综合评估。提供的信息应保证完整、准确、即时，不存在故意隐瞒、欺骗等行为。提供的信息应有详细的日志记录。移动应用软件集成SDK时，应保存引入时从SDK提供方获得的信息，包括但不限于：

a） SDK的开发者和运营者的必要信息。

b） SDK的安全性自评估报告和安全能力说明。

c） SDK应提供的安全反馈机制，明确告知安全事件及应急响应反馈渠道。

d） SDK的基本适用信息，例如在不同操作系统或操作系统版本下的使用建议。

e） SDK的基本功能说明，避免存在后门等问题。

f） SDK是否具有网络通信功能，若存在网络通信功能及其功能目的。

g） SDK是否具备单独为用户提供的登录或其他可输入个人信息界面的相关功能

h） SDK开发者或运营者如使用其他第三方代码或SDK的，应提供包括第三方代码或SDK名称，提供方或来源、使用的版本、采用的软件协议、有无已知安全漏洞等必要信息。

i） SDK开发者或运营者如需要通过应用软件间接获取个人信息，应向集成SDK的应用软件提供方提供个人信息处理的相关信息。例如收集、使用个人信息的目的、方式、范围及信息共

享机制等。应提供个人信息安全规范的管理相关要求信息。例如SDK提供方的用户协议，隐私政策，个人信息管理事件报告投诉接口人等信息。

j） SDK开发者或运营者如需要不通过应用软件而直接获取个人信息，应单独向SDK使用者提供个人信息处理的相关信息。例如收集、使用个人信息的目的、方式、范围及信息共享机制等。应提供个人信息安全规范的管理相关要求信息。例如SDK提供方的用户协议，隐私政策，个人信息管理事件报告投诉接口人等信息。

k） SDK提供方如直接调用或使用终端权限的，应向集成SDK的应用软件提供方提供权限调用的相关信息，包括但不限于目的、方式、范围等信息。

（3） SDK提供方与应用软件提供方在集成SDK前，若达成显式合同许可的，SDK提供方与应用软件提供方应完整实现其安全职责，若双方存在重大变更时，应重新达成合同许可。

（4） SDK提供方如存在与应用软件提供方共同个人信息收集使用或SDK提供方未通过应用软件而单方面收集个人信息行为时，应签订显式合同许可，明确其全生命周期中个人信息保护措施和义务。

5.2 权限申请使用要求

（1） SDK提供方申请、使用权限时，应满足最小、合理、必要原则。

（2） 移动应用软件提供方应在收集使用个人信息规则中声明其集成的SDK所申请的权限及功能目的。

（3） SDK提供方应在其网站或集成相关文档中声明所申请的权限列表及功能目的，如存在申请危险权限，则应公开声明功能必要性以及缺少该权限所导致的功能限制。

5.3 代码安全要求

（1） SDK提供方应保证提供的版本为现行稳定版，无已知安全漏洞和业务逻辑漏洞，不包含恶意代码，不包含静态代码扫描出的常见安全问题。

（2） SDK应单独或者与应用软件集成时采取代码混淆等安全技术保护源代码安全。

（3） 若SDK与应用软件间交互使用接口形式，SDK与应用软件都应对调用入口增加鉴权机制。

（4） 若SDK与应用软件间使用某种接口形式，SDK应对不同应用软件的上下文进行环境隔离，防止跨应用的信息泄漏或完整性破坏风险。

5.4 行为安全要求

（1） SDK提供方在无相关业务场景或无用户授权情况下不应主动进行后台唤醒或被其他应用软件唤醒。

（2） SDK提供方若主动调用系统API或进行后台其他敏感行为，应留存日志记录。

（3） SDK提供方不应在未经应用软件允许的情况下进行更新升级。

（4） SDK提供方不应在未经应用允许的情况下进行热修复或者动态加载组件。

（5） SDK提供方不应在应用和用户未知的情况下，唤醒其他处于静置状态的应用软件。

（6） SDK提供方不应在未经用户同意的情况下通过技术措施读取其他应用软件内的用户数据。

（7） SDK提供方不应在未经用户同意的情况下读取移动智能终端上的用户个人信息。

（8） SDK提供方不应以超出保持相关功能所必需的频次读取移动智能终端上的用户个人信息。

（9） SDK提供方不应探测、利用APP获取超过功能服务所必需的敏感权限。

（10） SDK提供方不应尝试进行命令执行或获取Root权限，不应在应用中尝试执行Root命令等。

5.5 传输安全要求

（1） SDK提供方不应存在未经用户同意的情况下向服务器传输用户个人信息。

（2） SDK提供方在数据传输过程中应使用安全传输协议传输如HTTPS协议等。

（3） SDK提供方应在传输过程中对用户个人敏感信息或敏感数据单独进行加密。

（4） SDK提供方若使用本地服务器的技术架构和方案，应保证本地服务器与远程服务器通信安全。

5.6 日志安全要求

（1）SDK提供方输出日志记录如包含用户个人敏感信息或敏感数据，应单独加密。

5.7 存储安全要求

（1） SDK提供方如在本地存储用户个人敏感信息或敏感数据，应加密存储。

（2） SDK提供方如在服务器保存用户个人敏感信息或敏感数据，应符合相关数据保护要求。

5.8 个人信息收集使用要求

SDK提供方在个人信息收集使用层面，应满足如下基本原则。

合理性原则：SDK提供方收集使用个人信息时，收集使用个人信息的目的、方式和范围应在其功能范围内。

最小化原则：SDK提供方收集使用个人信息时，应最小化收集使用个人信息，同时尽量采取本地方式处理个人信息。

透明性原则：SDK提供方收集使用个人信息时，应公开其收集使用个人信息的种类、目的、频次、时机、场景以及触发条件。

必要性原则：SDK提供方收集使用个人信息时，满足合理性原则，但超出移动应用软件提供者集成的实际需求之外，应适当删减。

（1） SDK提供方应为集成其SDK的应用软件提供方提供完整、准确、及时的个人信息处理相关资料。如有重大变更，则应及时通知应用软件开发者或运营者。如影响终端用户，则双方应合作履行个人信息安全规范所规定义务，向用户告知并重新征得用户同意等

（2） SDK提供方所单独处理的个人信息完全是本地处理，SDK提供方不作为个人信息控制者。此时，SDK提供方，应保证其控制范围内个人信息的本地安全处理，包括保证个人信息的机密性、完整性、不被未授权访问等。

（3） SDK提供方与应用软件提供方共同本地处理个人信息，各自保证其控制范围的个人信息收集使用安全，包括个人信息的机密性、完整性、不被未授权访问等。

（4） 应用软件提供方委托SDK提供方通过相应SDK收集和处理来自应用软件个人信息的，应用软件提供方应当保证收集和处理的个人信息的安全性。

a） 所有处理应符合《个人信息安全规范》的处理原则和要求。

（5） 应用软件提供方和SDK提供方共同通过相应SDK收集和处理的来自应用软件个人信息的，SDK提供方与应用软件提供方作为个人信息共同控制者，共同保证其收集和处理的个人信息的安全性。

a） 应用软件应向用户明示告知共同控制收集使用的个人信息。

b） 所有处理应符合《个人信息安全规范》的处理原则和要求。

（6） SDK提供方单独收集使用个人信息信息，应用软件提供方未委托或未知SDK提供方收集、使用个人信息的行为，或应用软件提供方通过技术措施为SDK提供方提供过个人信息，但应用软件提供方并未存储或处理相关信息，无相关信息备份。则应由SDK提供方保证其收集使用的个人信息的安全性。

a） SDK提供方若存在单独用户界面交互形式，应向用户明示其单独控制的个人信息，其透明性应满足用户可清晰得知数据控制者与应用软件运营者并非同一主体。并征得用户同意。

b） SDK提供方若不存在单独用户界面交互形式，应通过应用软件提供方向用户明示其单独控制的个人信息，其透明性应满足用户可清晰得知其数据控制者与应用软件运营者并非同一主体。并征得用户同意。

c） 应用软件提供方应为SDK提供方提供展示用户交互的便利。

d） 所有处理应符合《个人信息安全规范》的处理原则和要求。

（7） SDK提供方读取移动智能终端上的用户个人敏感信息如短信、通讯录、通话记录、日历等时，SDK提供方应保留相关日志，应用软件应提供良好的交互方式向用户提示。

（8） SDK提供方与集成其SDK的应用软件约定共享用户信息之外，不应私自收集使用其他的用户个人信息。

附录 A

（规范性附录）

标准修订历史

修订时间	修订后版本号	修订内容

附录 B

（资料性附录）

参考文献