软件绿色联盟应用体验标准2.0

安全标准

软件绿色联盟

Software Green Alliance

编制单位:软件绿色联盟·技术与标准工作组

2018年6月

修订记录

日期	修订内容
2017年5月15日	安卓绿色联盟应用体验标准1.0发布
2018年7月17日	1) 修订 4.4 行为规范 2) 修订 5.1 Manifest和权限使用安全规范 3) 增加 5.7 隐私安全
2019年6月27日	联盟在第三届理事会议宣布正式更名为“软件绿色联盟”，本标准同步更名为“软件绿色联盟应用体验标准2.0 安全标准”。

目 次

前 言

本标准由软件绿色联盟技术与标准工作组提出并归档

本标准起草单位：软件绿色联盟

本标准主要起草人：阿里巴巴、百度、华为、腾讯、网易、360、TAF协会、爱加密

标准名称

1 范围

本标准规定了Android应用的质量、应用体验标准。

本标准适用于Android应用软件的设计、开发及检测。

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。

《软件绿色联盟应用体验标准 1.0 - 安全标准》

3 术语、定义和缩略语

3.1 术语和定义

3.1.1 Activity

Activity是Android组件中最基本也是最为常见用的四大组件之一，是一个应用程序组件，提供一个屏幕，用户可以用来交互为了完成某项任务

3.1.2 Intent

intent主要是解决Android应用的各项组件之间的通讯。Intent负责对应用中一次操作的动作、动作涉及数据、附加数据进行描述，Android则根据此intent的描述，负责找到对应的组件，将 intent传递给被调用的组件，并完成组件的调用。

4 基础安全标准

4.1 安装，运行及卸载

应用在用户未授权情况下，不能进行程序下载、安装、或升级操作；

应用在用户未授权情况下，不能执行自启动操作；

应用在用户强制关闭或退出后，不能继续占用系统资源；

应用中不能包含反卸载操作；

4.2 功能使用

应用在用户未授权情况下，不能执行拨打电话、发送短信等操作；

应用在用户未授权情况下，不能执行摄像、录音、截屏等操作；

应用在用户未授权情况下，不能打开或关闭如WiFi、蓝牙、GPS等；

4.3 数据操作

应用在用户未授权情况下，不能读写用户短信、联系人等隐私数据；

应用在用户未授权情况下，不能收集或上报用户设备、系统及应用程序信息；

应用在用户未授权情况下，不能修改系统配置等资源文件；

应用在用户未授权情况下，不能修改其他应用程序的权限、数据等；

4.4 行为规范

应用在用户未授权情况下，不能进行消费操作；

应用不能包含故意破坏用户使用体验、阻碍用户正常使用手机或应用的任何行为；

应用中不能包含任何侵犯用户知情权、选择权的恶意行为

应用在用户未授权情况下，不能利用漏洞等方式获取系统控制权限，进行非授权操作；

如无必要的使用场景，应用不能在桌面、锁屏和其他应用上，弹出悬浮窗、自定义后台Toast、后台弹出Activity等骚扰用户的行为；

如无必要的使用场景，应用不能发送无法删除的常驻通知；

应用不能弹出、显示影响用户体验的广告，如抬头、强制插屏、侧边等；

应用不能引导用户开启开发者选项，禁止引导用户开启USB调试模式；

4.5 其他标准

应用不能包含病毒、木马；

应用不能包含漏洞、后门；

应用不能包含国家法律禁止的内容，包括但不限于色情，赌博，或任何危害国家安全的信息；

应用不能包含其他任何形式损害用户利益及资产的行为；

应用不能通过热补丁，引入恶意行为和不符合本标准的行为；

5 开发安全标准

5.1 Manifest 和权限使用安全规范

1）权限管理。权限使用满足最小化原则：

- ✓ 不申请不需要使用的权限，为自定义权限设置合理的安全保护级别；
- ✓ 应用申请的权限，都必须有明确、合理的功能和使用场景；
- ✓ TargetSdkVersion>=23，必须适配Android M及以后版本的动态权限机制。
- ✓ 对于非核心权限，应用不能在权限动态弹框授权提示被用户拒绝后，强制要求用户开启，包括但不限于：（1）应用退出；（2）弹框提醒用户打开>=2次；

2）功能项管理。关闭不需要及有风险的功能选项，如数据备份功能、调试功能；

3）组件管理。组件声明的合理性，避免导出不需要外部调用的组件，如需导出应设置合理的权限保护；

5.2 应用编码安全规范

5.2.1 基础编码安全规范

1）保证开发环境的安全性，如使用官方渠道下载的开发工具；
2）避免硬编码关键数据，如加密密钥、后端服务器敏感信息等；
3）应用代码净化，代码逻辑优化、剔除应用中的死代码块；
4）统一的日志管理接口，避免在日志中记录敏感信息；
5）应用发布之前，关闭调试接口和调试日志。

5.2.2 系统 API 使用安全规范

1）使用官方推荐版本的API接口，不使用系统废弃的API
2）熟悉并遵从安全规范，避免遗漏安全限制操作，引入安全风险；
3）对关键操作身份校验和权限检查；

5.2.3 第三方代码使用安全规范

1）代码评估。来源可靠性评估、代码质量评估、潜在安全风险评估；
2）权限控制。确认引入代码所需使用的权限最小化；
3）更新维护。关注代码的安全动态和版本更新情况，及时修复安全问题，更新代码；
4）安全保护。对引入的代码进行混淆，防止攻击者针对性的攻击；

5.2.4 代码保护安全规范

1）代码混淆。提高攻击者代码分析难度；
2）加固保护。使用自研或者第三方加固系统进行应用加固，进行代码隐藏和加密保护；

5.3 数据安全规范

5.3.1 数据加密安全规范

1) 数据密文和加密密钥应存放在不同的位置；
2) 密钥存储模块应具备防调试及反编译的能力；
3) 密钥数据应分散存储，为获取密钥密文增大难度

5.3.2 数据存储安全规范

1) 应用程序关键数据应该存放在私有目录下，并设置合理的访问权限；
2) 应用程序中的隐私数据应加密存储。用于加密的密钥应妥善保存；
3) 禁止程序运行日志中包含有用户敏感数据、程序调试数据等；

5.3.3 数据使用安全规范

1) 数据合法性保护。控制用户输入数据的类型、长度，进行恶意代码过滤等；
2) 数据完整和有效性保护。对于接收到的外部数据、加载的外部文件，进行完整、有效性性检查；

5.4 通信安全

5.4.1 本地通信安全

1) intent数据安全。避免在intent包含用户敏感数据，从intent中获取数据时加入必要的异常处理；
2) intent scheme url 协议安全。使用过程中加入安全限制，防止UXSS等安全问题；
3) 组件调用方式安全。避免通过隐式方式进行调用组件，防止组件劫持；

4) 本地socket通信安全。避免是使用socket方式进行本地通信，如需使用，localhost端口号随机生成，并对端口连接对象进行身份认证和鉴权；

5.4.2 远程通信安全

1) 使用https代替http进行通信，并对https证书进行严格校验；
2) 避免进行远程端口开发通信，如需使用，需要对端口连接对象进行身份认证和鉴权；

5.5 业务安全

5.5.1 认证和授权

1) 认证和授权过程应在服务器端完成，避免客户端绕过问题；
2) 对于涉及敏感信息的服务，每次使用前需进行身份认证；
3) 控制登录凭证token有效期，通信过程中进行token鉴权；
4) 避免在终端设备上使用不安全的方法来存储用户名、口令及其它登录凭证；
5) 用户密码需要使用强不可逆的加密算法加密后传输，并引入salt，提高破解难度；
6) 账户号和终端设备信息进行绑定，防止终端模拟攻击；

5.5.2 业务逻辑及数据安全

1) 条件判断。确保逻辑过程中前置判断条件的有效性、不可绕　过性，防止攻击者进行数据修改绕过安全限制；
2) 逻辑设计。确保业务逻辑设计、分支条件及边界条件处理的正确性和完备性，防止不可控执行流程；
3) 工作分配。确保服务端和客户端分工正确，防止一些应该放在服务

端的校验工作设置在了客户端，造成权限校验绕过；

4) 业务数据。关键业务数据防篡改、防伪造、防重放；

5) 短信验证码安全。禁止验证码回传行为，验证码至少6位,同时严格限定验证码时效；

5.5.3 业务运维安全

1) 业务风险监控、预警、异常处理预案；

2) 安全动态跟踪及预警、安全事件排查、漏洞修复；

5.6 运行环境安全

1) 运行期重打包检测；

2) 模拟器运行环境检测；

3) 调试、注入操作监控；

4) root环境运行检测；

5.7 隐私安全

1) 涉及到应用下载软件、对用户系统或软件升级等修改用户个人空间的行为，须得到用户的同意

2) 收集或使用个人数据前，须明确提示用户，并获得用户的明示同意，并且允许用户随时关闭对个人数据的收集和使用

3) 默认禁止收集数据主体的敏感个人数据，除非业务必需（如：运动健康类业务）或为了满足法律与监管机构要求可收集和处理（含profiling），并且同意应该单独收集

4) 应提供对用户的同意和撤销同意行为进行记录的机制

5) 隐私声明内容发生变化时，须告知用户查看并获得用户同意

6) 个人数据收集范围、使用目的不得超出隐私声明，且遵循最小化原则，当个人数据的采集范围、使用目的发生变更时，应及时更新隐私声明

7) 于存储个人数据的系统，需对存储的个人数据定义存留期

8) 数据主体撤销同意之后，产品必须禁止继续收集和处理其相应个人数据

9) 将数据主体个人数据提供给第三方前，必须获得数据主体的同意

10) 推送的内容（含广告）必须是符合政治、法律和宗教要求，并且推送频度不能干扰用户正常使用

11) 第三方应用软件调用移动智能终端敏感功能时，应先获得用户明确同意

12) 第三方应用软件对用户数据操作时，应先获得用户明确同意

13) 应用软件不得申请和调用与提供服务无关的终端功能