软件绿色联盟应用体验标准3.0

安全标准

（公示版）

编制单位:软件绿色联盟·技术与标准工作组

2019年7月

目 录

前 言 4
标准名称....4
1 范围....4
2 规范性引用文件....4
3 术语、定义和缩略语....4
3.1 术语和定义....4
3.1.1 Activity....4
3.1.2 Intent 5
3.1.3 个人数据....5
3.1.4 敏感个人数据....5
3.1.5 匿名化....5
4 应用行为安全标准....6
4.1 基本要求....6
4.2 安装....6
4.3 启动....6
4.4 运行....6
4.4.1 隐私....6
4.4.2 权限....8
4.4.3 恶意行为....10
4.4.4 骚扰行为....10
4.5 退出....10
4.6 卸载....10
4.7 其他....10
5 应用开发安全标准....11
5.1 权限使用安全规范....11
5.2 应用编码安全规范....12
5.2.1 基础编码安全规范....12
5.2.2 系统API使用安全规范 12
5.2.3 第三方代码使用安全规范....12
5.2.4 代码保护安全规范....12
5.3 数据安全规范....13

5.3.1 数据加密安全规范.....13
5.3.2 数据存储安全规范.....13
5.3.3 数据使用安全规范.....13
5.4 通信安全.....13
5.4.1 本地通信安全.....13
5.4.2 远程通信安全.....14
5.5 业务安全.....14
5.5.1 认证和授权.....14
5.5.2 业务逻辑及数据安全.....15
5.5.3 业务运维安全.....15
6 修订记录.....15

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、中国泰尔实验室、新浪、爱加密、360、安天

标准名称

1　范围

本标准旨在提升应用的质量和体验。

本标准适用于应用软件的设计、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 3.0 - 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是系统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，应用则根据此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。

3.1.3 个人数据

与一个身份已被识别或者身份可被识别的自然人（“数据主体”）相关的任何信息。身份可识别的自然人是指其身份可以通过诸如姓名、身份证号、位置数据等识别码或者通过一个或多个与自然人的身体、生理、精神、经济、文化或者社会身份相关的特定因素来直接或者间接地被识别。

个人数据包括：自然人的email地址、电话号码、生物特征（指纹）、位置数据、IP地址、医疗信息、宗教信仰、社保号、婚姻状态等。

3.1.4 敏感个人数据

敏感个人数据是个人数据的一个重要子集，指的是涉及数据主体的最私密领域的信息或者一旦泄露可能会给数据主体造成重大不利影响的数据。欧盟等国家和地区法律定义的敏感个人数据包括种族、政治观点、宗教和哲学信仰、工会成员资格、基因数据、生物信息、健康和性生活状况、性取向等。根据业界最佳实践，华为公司定义的敏感个人数据还包括可与自然人身份相关联的银行卡号、身份证号、护照号、口令等。敏感个人数据的处理需要更多更严格的保护措施。

3.1.5 匿名化

是对个人数据进行不可逆改变的过程，个人数据匿名化处理后将无法直接或间接地识别数据主体或者识别需要不合理的耗费大量的时间，费用和精力。

4 应用行为安全标准

4.1 基本要求

1) 数据收集遵循合法、正当、必要、透明的原则。
2) 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。
3) 不能包含恶意行为和欺骗性行为。
4) 不能包含病毒、木马、漏洞、后门。
5) 不能诱导、欺骗用户执行有损系统和应用安全的操作，包括但不限于下载或安装系统root工具，激活设备管理器选项，开启辅助功能等。

4.2 安装

1) 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。
2) 禁止胁迫、恐吓、强迫、诱导用户下载和安装其他应用。
3) 禁止为安装恶意软件提供链接或其他引导。
4) 禁止在未明确告知用户的情形下，诱导用户安装应用。
5) 禁止应用安装后自动在桌面添加多图标。
6) 禁止应用程序在安装后首次启动时，要求用户完成积分任务才能使用应用的基本功能，否则应用强制退出。

4.3 启动

1) 应用在用户未授权情况下，不能执行自启动操作。

4.4 运行

4.4.1 隐私

应用应遵循的相关法律法规的要求，包括国家和行业标准，监管部门要求等。

隐私保护设计要保证对用户充分透明、给予用户充分的可知可控的能力，并赢得用户的信任。

合法、正当、透明：个人数据应当以合法、正当、对数据主体透明的方式被处理。

目的限制：个人数据应当基于具体、明确、合法的目的收集，不应以与此目的不相符的方式作进一步处理。

数据最小化：个人数据应与数据处理目的相关，且是适当、必要的。尽可能对个人数据进行匿名或化名，降低对数据主体的风险。

准确性：个人数据应当是准确的，并在必要的情况下及时更新。根据数据处理的目的，采取合理的措施确保及时删除或修正不准确的个人数据。

存储期限最小化：存储个人数据不超过实现数据处理目的所必要的期限。

完整性与保密性：根据现有技术能力、实施成本、隐私风险程度和概率采取适度的技术或组织措施确保个人数据的适度安全，包括防止个人数据被意外或非法毁损、丢失、篡改、未授权访问和披露。

可归责：数据控制者须负责且能够对外展示遵从上述原则。

1） 通知

- 在收集个人数据之前应提供隐私声明。
- 如果收集个人数据类型、使用目的、数据控制者发生变化，应重新通知用户。
- 隐私声明可供用户随时查阅，查阅方式应易于操作。
- 隐私声明的语言简洁明了，使用当地的官方语言。
- 隐私声明中须说明：

-业务功能及每个业务功能收集的数据类型和用途

-个人数据存储地点和存储时限

-数据披露给第三方的场景和数据类型

-数据跨境转移的场景

-数据主体权利

-应用运营者公司名称、注册地址、个人信息保护相关负责人的联系方式

-隐私通知更新日期

2） 选择和同意

- 收集个人数据前，需获得用户的同意。

- 收集敏感个人数据前，需单独获得用户的明示同意。
- 应提供用户撤销同意的方式，操作方式应简单易懂且易于操作，用户撤销同意后，停止收集个人数据。

3) 收集

- 个人数据的收集应满足最小化原则，收集的范围、使用目的不得超出隐私声明。
- 应用禁止使用IMEI、SN等物理识别码作为唯一设备标识符，避免长期对用户跟踪的行为。
- 群体数据分析的场景下避免收集个人数据，应采用数据最小化技术，如对个人数据进行泛化，匿名化，差分隐私。

4) 使用、留存和处置

- 对存储的个人数据定义留存期，到期后需删除或者匿名化个人数据。

5) 向第三方披露

- 个人数据提供给第三方前，必须获得数据主体的同意。

6) 数据主体访问

提供注销账号的途径，并在用户注销账号后删除或者匿名化个人数据。

提供用户查询、更正、删除个人数据的途径。

7) 数据跨境转移

- 个人数据跨境转移前，必须获得数据主体的同意。

4.4.2 权限

1) 应用的API Level不能低于26（TargetSdk Version不能低于26），推荐设置API Level为28。
2) 应用申请的权限，都必须有明确、合理的使用场景和功能说明。确保用户能够清晰明了地知道应用所申请权限的场景、用途、目的等信息；禁止诱导、误导用户授权。应用使用权限必须与申请所述一致。
3) 权限申请遵循最小化原则，应用只申请业务功能所必要的权限。
4) 应用在安装后首次启动的时候，避免频繁弹框申请多个权限，通过一

次弹窗批量申请核心功能所需权限；其他敏感权限需要在用户使用对应业务功能时动态申请。

5) 应用不得申请权限直接拨打电话、发送短信。只有在用户主动将应用注册为默认短信、电话程序的情况下，应用向用户申请拨打电话、发送短信权限。

6) 严格控制应用申请位置权限，除导航、运动类应用可申请持续获取位置，其他类型应用程序禁止申请后台持续获取位置权限，仅在使用时获取位置。

7) 严格控制外部存储权限，应用存在读取外部存储上文件的用户功能时，才允许申请外部存储权限，其他场景禁止申请外部存储权限。

8) 避免使用硬件标识符（例如IMEI），改用其他可替代的方案，减少申请READ_PHONE_STATE权限。

9) 用户拒绝授予某个权限时，与此权限无关的其他业务功能应能正常使用。

10) 业务功能所需要的权限被用户拒绝、禁止后不能强制退出；不允许应用每次启动时都向用户申请，当用户再次使用此功能时向用户申请对应权限，向用户申请权限次数不超过3次。

11) 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。

12) 应用在用户未授权情况下，不能执行摄像、录音、截屏等操作。

13) 应用在用户未授权情况下，不能打开或关闭如Wi-Fi、蓝牙、GPS等。

14) 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。

15) 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。

16) 应用在用户未授权情况下，不能修改系统配置等资源文件。

17) 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。

18) 应用在用户未授权情况下，不能进行消费操作。

19) 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。

20) 应用在用户未授权情况下，不能在桌面创建桌面快捷方式。

4.4.3 恶意行为

1) 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。
2) 应用中不能包含任何侵犯用户知情权、选择权的行为。
3) 应用不能将广告伪装成应用功能误导消费者。
4) 禁止诱导、欺骗用户修改、关闭、卸载其他经营者合法提供的网络产品或者服务。
5) 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。

4.4.4 骚扰行为

1) 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。
2) 如无必要的使用场景，应用不能发送无法删除的常驻通知。
3) 广告只能在其本身所属的应用内展示，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。

4.5 退出

1) 应用在用户强制关闭或退出后，不能继续占用系统资源。
2) 禁止应用程序之间互相作为守护程序；在用户退出应用时，通过其他应用程序后台唤醒，导致无法彻底退出。

4.6 卸载

1) 应用中不能包含反卸载操作。
2) 应用的私有数据必须写到自己的私有文件夹，卸载应用时必须清除干净。 只有输出后要共享出去的数据，比如图片、音乐、录像或其他需要共享给其他应用的文件和数据，才放到公共文件夹。

4.7 其他

1) 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。

2) 应用不能通过在应用内提示并提供下载的方式进行程序升级，应用程序的升级应该通过应用市场进行。除应用版本有严重问题，用户必须升级到最新版本才能使用应用核心功能的情况下，禁止强制用户升级应用。
3) 应用不能引导用户对手机进行ROOT操作。

5 应用开发安全标准

5.1 权限使用安全规范

1) 应用（包括引用的第三方SDK）所需权限必须在权限说明中逐个声明。
2) 应用避免因为引入第三方SDK，导致过度申请权限和冗余权限。
3) 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。
4) 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) 应用通过敏感权限获得的数据和能力，禁止以自定义接口向外提供。
6) 应用如需访问其他应用共享的文件，应该使用SAF框架，由用户选择对应文件，而不应该申请外部存储权限直接去读取。
7) 必须对涉及敏感数据、敏感操作的对外交互组件设置访问权限。
8) 调用会抛SecurityException的接口，需要捕获SecurityException，防止应用闪退。
9) 除默认短信和默认电话应用外，其他应用禁止申请SMS和CALL_LOG权限组内的所有权限。
10) 禁止应用申请CALL_PHONE权限去直接拨打电话(Intent.ACTION_CALL)。
11) 禁止应用申请SEND_SMS权限去直接发送短信。
12) 应用自定义权限必须严格定义，确保完整、清晰、准确，并为权限配置合理的保护级别。
13) 应用自定义权限名，建议以应用包名为前缀，防止与系统或其他应用

定义的权限重名。

14) 禁止一个权限保护多类数据和多种能力，禁止定义保护范围重叠的新权限。

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) 对于不同版本中系统限制使用权限相关API，应说明不同版本中可能存在的隐私合规问题。
3) 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。
4) 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） 服务端对高敏感数据存储不能明文存储，应采用高安全等级的加密算法，密钥控制在最小范围，防止被拖库后破解。
2） 数据密文和加密密钥应存放在不同的位置。
3） 密钥存储模块应具备防调试及反编译的能力。
4） 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。
4） 建议应用程序采用沙箱技术，同时建议一切穿透应用沙箱的行为都使用权限来管控。

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。
7) 涉及敏感操作的业务功能，需要通过多因子身份认证提升安全性（短信验证码、软硬件token、生物特征等）。

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。

6 修订记录

日期	修订内容	修订主体
2017年5月	安卓绿色联盟应用体验标准1.0发布	
2018年7月	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7月	1) 更名为《软件绿色联盟应用体验标准3.0_安全标准》 2) 部分规范文字描述更改 3) 修订 4.1 基本要求 4) 修订 4.2.2 权限 5) 修订 4.6 退出 6) 修订 5.1 权限使用安全规范	