**Android客户端适配9.0方案**

目录

Section 1: 前言 1-4

1 概念 1-4

2 读者 1-4

3 参考文档 1-4

Section 2: 技术方案 2-5

1 所有应用的行为变更 2-5

1.1 非SDK开放接口 2-5

1.2 加密提供商变更 2-6

1.3 后台应用访问受限 2-6

1.4 权限变更 2-6

1.5 Apache HTTP API 使用变更 2-8

1.6 强制执行 FLAG\_ACTIVITY\_NEW\_TASK 2-8

1.7 电源管理优化 2-8

2 针对Api 28+ 的行为变更 2-9

2.1 前台服务权限新增 2-9

2.2 构建序列号弃用 2-9

2.3 多进程Webview 2-9

2.4 默认采用Https进行数据访问 2-10

# 前言

## 概念

主要是Android客户端适配9.0时的注意事项及主要更改点，所列技术点并不全面，更详细的技术文档请参照谷歌官方文档。

## 读者

xx

## 参考文档

谷歌官方文档

<https://developer.android.google.cn/about/versions/pie/>

# 技术方案

## 所有应用的行为变更

### 非SDK开放接口

在Android9.0环境中，对于非 SDK API 里面的部分名单来说，就算在不修改 targetSdkVersion 的前提下，不管是直接、反射还是通过 JNI 调用都会造成调用失败、抛NoSuchFieldException或 NoSuchMethodException 等严重后果，该行为影响范围波及所有调用此接口的应用。

非 SDK API 名单总共分为三类：light grey list （浅灰名单）、dark grey list （深灰名单）、dark list（黑名单）。



查看这些名单的网址：<https://android.googlesource.com/platform/frameworks/base/+/master/config/>

扫描项目中的非SDK名单调用列表：

<https://android.googlesource.com/platform/prebuilts/runtime/+/master/appcompat>

**备注：扫描插件的使用详见上面链接中的README.txt**

### 加密提供商变更

影响的提供商有Crypot、BC，以下写法会抛出NoSuchProviderException、NoSuchAlgorithmException异常。

SecureRandom.getInstance("SHA1PRNG", "Crypto")

Cipher.getInstance("AES/CBC/PKCS7PADDING", "BC") or

Cipher.getInstance("AES/CBC/PKCS7PADDING", Security.getProvider("BC"))

**备注：通过查看源码发现，系统会维护一份提供商的列表，根据传入的第二个参数查询出加密的算法提供商，如果找不到会抛出异常。**

### Apache HTTP API 使用变更

要继续使用 Apache HTTP 客户端，以 Android 9 及更高版本为目标的应用可以向其 AndroidManifest.xml 添加以下内容：

<uses-library android:name="org.apache.http.legacy" android:required="false"/>

**备注：拥有最低 SDK 版本 23 或更低版本的应用需要 android:required="false" 属性，因为在 API 级别低于 24 的设备上，org.apache.http.legacy 库不可用。 （在这些设备上，Apache HTTP 类在 bootclasspath 中提供。）**

### 强制执行 FLAG\_ACTIVITY\_NEW\_TASK

在 Android 9 中，不能从非 Activity 环境中启动 Activity，除非传递 Intent 标志 FLAG\_ACTIVITY\_NEW\_TASK。 如果尝试在不传递此标志的情况下启动 Activity，则该 Activity 不会启动，系统会在日志中输出一则消息。

**备注：在 Android 7.0（API 级别 24）之前，标志要求一直是期望的行为并被强制执行。 Android 7.0 中的一个错误会临时阻止实施标志要求。**

### 电源管理优化

Android 9 引入了一项新的电池管理功能，即应用待机群组。 应用待机群组可以基于应用最近使用时间和使用频率，帮助系统排定应用请求资源的优先级。 根据使用模式，每个应用都会归类到 五个 优先级群组之一中。 系统将根据应用所属的群组限制每个应用可以访问的设备资源：

1. 确保应用在各种模式下能够正常工作
2. 可以让用户手动把应用加入白名单中，解除系统限制。

**备注：具体电源管理分类、如何调试、如何加入白名单等参考**

[**https://developer.android.google.cn/about/versions/pie/power**](https://developer.android.google.cn/about/versions/pie/power)

## 针对Api 28+ 的行为变更

### 前台服务权限新增

针对 Android 9 或更高版本并使用前台服务的应用必须请求 FOREGROUND\_SERVICE 权限。 这是普通权限，因此，系统会自动为请求权限的应用授予此权限。

如果针对 Android 9 或更高版本的应用尝试创建一个前台服务且未请求 FOREGROUND\_SERVICE，则系统会引发 SecurityException。

### 默认采用Https进行数据访问

也就是运行在9.0 系统的应用没有做Https适配的话，所有Http无法访问，解决这个问题有两种方案可以参考（两种选择一个即可）

1. 全局关闭检查
2. 未特定域名关闭检查（需谨慎排查、包括三方SDK）

**第一步Application节点配置xml文件**

<application android:networkSecurityConfig="@xml/network\_security\_config">

<!-- ... -->

</application>

**第二步（xml 文件network\_security\_config配置）**

全局配置

<network-security-config>

<base-config cleartextTrafficPermitted="true">

<trust-anchors>

<certificates src="user"/>//信任用户自己安装的证书

<certificates src="system"/>

</trust-anchors>

</base-config>

</network-security-config>

局部配置

<network-security-config>

<domain-config cleartextTrafficPermitted="false">

<domain includeSubdomains="true">secure.example.com</domain> // 域名

</domain-config>

</network-security-config>

**备注：xml配置语法较多 具体查看官方文档** <https://developer.android.google.cn/training/articles/security-config>