

腾讯云应用安全

应用安全

产品文档



腾讯云

## 【版权声明】

©2013-2017 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

## 【商标声明】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

## 【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。

## 文档目录

文档声明.....	2
应用安全.....	4
购买指导 .....	4
使用说明 .....	6
常见问题.....	13
应用加固.....	13
兼容性测试 .....	19
安全测评.....	20
安全软键盘 .....	22
崩溃检测.....	23
白盒密匙.....	24
盗版监控.....	25

应用安全

## 购买指导

### 购买指导

目前应用加固的购买分为基础版，专业版，私有服务版三种，每一个版本的功能与参考价格如下：

类别	功能	基础版	专业版	私有化服务版	
反编译保护	DEX反编译保护	APK防反编译	APK防反编译	APK防反编译	
		壳加密算法保护	壳加密算法保护	壳加密算法保护	
		AndroidManifest.xml 防反编译	AndroidManifest.xml 防反编译	AndroidManifest.xml 防反编译	
		DEX文件整体加固保护	DEX文件整体加固保护	DEX文件整体加固保护	
			DEX类抽取加固	DEX类抽取加固	
			DEX虚拟化加固 (VM P)	DEX虚拟化加固 (VM P)	
	SO反编译保护			SO库加壳保护	SO库加壳保护
					SO库内存动态清除
					SO库与应用绑定保护
					高级SO混淆保护
				SO库字符串加密	
防篡改保护	APK防篡改保护		APK防二次打包保护	APK防二次打包保护	
			APK签名文件校验保护	APK签名文件校验保护	
	源代码防篡改保护	DEX文件防篡改	DEX文件防篡改	DEX文件防篡改	
			SO库防篡改	SO库防篡改	
	资源防篡改保护		assets资源防篡改	assets资源防篡改	
			res资源防篡改	res资源防篡改	
			raw资源防篡改	raw资源防篡改	
		配置文件防篡改	配置文件防篡改		
防调试保护	防调试保护		防模拟器保护	防模拟器保护	
		加固壳防动态调试	加固壳防动态调试	加固壳防动态调试	
			防线程动态调试保护	防线程动态调试保护	

			防进程动态调试保护	防进程动态调试保护
			防jdpw调试	防jdpw调试
			防注入保护	防注入保护
		防内存dump保护	防内存dump保护	防内存dump保护
		防内存数据读取	防内存数据读取	防内存数据读取
			防内存数据修改	防内存数据修改
数据与资源保护	资源防窃取保护		assets资源防窃取	assets资源防窃取
			res资源防窃取	res资源防窃取
			raw资源防窃取	raw资源防窃取
				SLL证书防窃取
	本地数据保护		本地databases目录 数据库文件加密	本地databases目录 数据库文件加密
				本地webview数据库 加密
				本地sharepreference 数据加密
		防日志泄漏	防日志泄漏	
			应用防截屏/录屏	
Unity游戏加固	Unity游戏加固		libmain.so加固	libmain.so加固
				libunity.so加固
				libmono.so加固
		免费	¥80,000元/年	按服务需求，面议价

**注意：**

基础版，使用通用的基础加固策略，可直接使用；

专业版，使用默认专业版加固策略，稳定可靠；若有定制策略需求，请直接联系我们；

私有化服务版，对于有明确需求的私有化部署客户，请直接联系我们！

服务电话：4009-100-100

## 使用说明

### 乐固服务概述

Android分发市场众多，针对应用的二次打包、逆向破解层出不穷。为此，乐固针对移动应用开发者，推出了应用加固服务。用户只需上传安装包（需已签名），就能自动进行应用加固。下载加固包后重签名即可免测发布，贴心保卫您的版权和收入。

### 乐固使用说明

#### 1. 上传应用

1) 从官网乐固产品介绍页中点击立即使用，进入控制台；



2) 进入控制台后，直接进入“应用管理”页面，点击“上传应用”按钮，上传开发者自主研发的apk文件。开发者需要上传已签名的apk，否则无法加固。



#### 欢迎使用腾讯云乐固服务

乐固为您的服务提供全方位安全服务，使用乐固还可以提高应用宝开发星级，享受应用宝审核、推广特权



3) 或者在左侧边栏

，点击进入“基础服务”的“加固应用”，进入后同样可以点击“上传应用”，上传开发者自助研发的apk文件。

开发者需要上传已签名的apk，否则无法加固。



### 欢迎使用应用加固

应用加固保护应用核心逻辑和代码安全，防破解、反逆向，拒绝盗版侵权。



2. 等待上传完成

乐固会在数分钟内完成您的应用加固上传，具体时间时具体应用情况有所不同。待加固完成后页面会自动刷新。



### 3. 选择服务

上传完成，确认应用信息。乐固为开发者提供安全加固及数据服务和其他可选择的应用体验，开发者可根据需求选择，勾选完成后，点击“提交”按钮。

[< 返回](#) | 选择服务

基本信息



应用名 YSDKDemo  
版本号 1.0.0  
文件名 sdk\_legu\_signed\_zipalign.apk  
包名 com.tencent.tmgp.yybtstsdm

选择服务

应用体检

漏洞扫描

探知程序漏洞，预防安全隐患



盗版监控

盗版追踪溯源，数据精准掌握



真机测试

解决适配难题 今日免费剩余1次



安全加固及数据服务

应用加固

拒绝盗版侵权，捍卫开发者利益



质量跟踪

一键接入bugly，跟踪异常数据



提交

4. 等待加固完成



大概需要8分钟，您可以先去进行其他操作，稍后再来查看  
 推荐您使用 [乐固自助加固](#) 工具，可自动加固、签名

### 5. 加固成功 下载加固包并重签名

加载成功后直接跳转到“应用加固”页面

应用加固 [噢噢App安装包...](#)

**加固结果**

加固成功

**应用已加固，可有效防盗版、反破解！**

加固会不可避免的破坏应用签名，为避免应用加固后无法安装，请务必按照下列流程对加固包进行重签名：

① [下载加固包](#) > ② [下载重签名工具](#) > ③ [对加固包进行重签名（需保持加固前后签名一致）](#) > ④ [发布重签名后加固包](#)

下载加固包

下载签名工具

---

**加固详情**

维度	加固前	加固后
腾讯开放平台特权	无特权	星级计划 +100 分，享受审核、曝光特权 <a href="#">查看详情</a>

1) 点击“下载加固包”可获取已加固后的安装包，但必须对加固包重签名后才能够发布，否则会导致应用安装失败。



2) 乐固官方向开发者提供了可进行本地签名工具。加固后，开发者点击“下载签名工具”即可下载乐固提供的PC端自助加固工具，获取对应的工具及使用说明文档。

名称	大小	压缩后大小
bin	183 909 194	65 715 850
README.txt	1 045	484
PC加固工具使用文档以...	555 996	502 083
LeguPC.exe	1 585 864	736 718

## 6. 多渠道打包

在应用分发过程中，开发者需要在APK配置文件AndroidManifest.xml内配置渠道信息，使得不同渠道发布的包能够具有标识该渠道包的能力。因此，乐固提供了PC工具，可进行多渠道打包，方便开发者快速进行多渠道打包。

加固完成后，点击“自助加固工具”，用户即可获取对应的工具及使用说明文档，下载后可在PC端工具直接实现应用加固、签名、多渠道打包。



工具下载

**Windows自助加固工具**

适用平台 Windows  
版本号 V2.0.2  
更新日期 2017-07-28  
功能说明 可自动加固、签名及多渠道打包，一键完成

下载

**Mac自助加固工具**

适用平台 MAC  
版本号 V2.0.2  
更新日期 2017-07-28  
功能说明 可自动加固、签名及多渠道打包，一键完成

下载

**批量签名工具**

适用平台 Windows  
版本号 2.0  
更新日期 2016-06-01  
功能说明 可批量签名，打多渠道包，无加固功能。

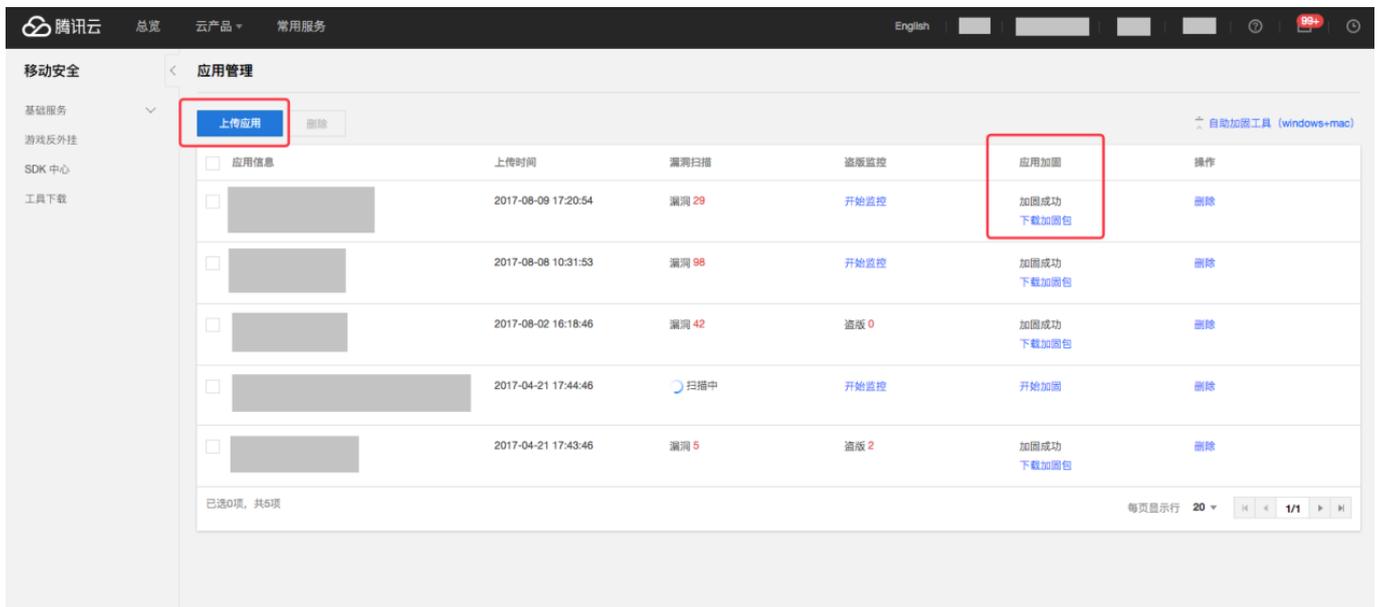
下载

## 7. 应用管理

加固完成后，可直接点击左侧“基础服务”边栏，进入应用管理。

可点击“上传应用”再次上传需要加固的apk。

同时可以对应用进行“漏洞扫描”、“盗版监控”、“下载加固包”、“删除”等操作。



## 常见问题

### 应用加固

#### 为什么要应用加固？

1. Android 应用使用 Java 语言编程，易被反编译，破译核心业务逻辑和算法；
2. Android 应用易被二次打包，插入病毒、木马、流氓广告等恶意代码；
3. Android

系统本身开源特性，以及移动应用承载的越来越多的核心业务，使其已成为黑客的主要攻击对象。

#### 加固对应用性能有什么影响？

腾讯云应用加固经过多年实践，已实现应用固后与加固前相比，性能影响极小，用户使用基本无感知。

#### 应用加固对兼容性有什么影响？

应用加固是基于加密、加壳技术对 App 进行保护。理论上对应用加固后的兼容性会产生一定影响。但腾讯云应用加固基于 12 亿终端的实践，以及每次加固后的兼容性测试服务，能够有效保证应用加固后的兼容性水平。

#### 不同类型应用的加固策略，都是一样的吗？

目前腾讯云提供免费和收费版本的应用加固服务，

1. 免费版本使用通用加固策略，保证基本的 App 安全，普遍适用于各种应用，稳定性和兼容性可靠。
2. 收费版本，是针对于应用自身的特性，及用户需要，专属加固策略，实现更高的 App 安全标准；同时，基于人工的加固策略审核，以及加固后的兼容性测试服务，可以更好的保证应用加固后的稳定性和兼容性。

#### 针对于手机游戏的 u3d、cocos2d 等引擎，可以加固吗？

腾讯云应用加固，针对于 u3d、cocos2d 引擎，有专用的加固方案，适用于付费版本。

## 什么是 debug 签名

Android 应用通过数字签名来标识应用程序的作者和应用程序之间的信任关系。

Android 的这个签名由应用程序的作者完成，并不需要权威的数字证书签名机构认证，只是用来让应用程序包自我认证的。Android 系统默认自动给应用程序签名，ADT 会自动使用 debug 密钥为应用程序签名，debug 密钥是一个名为 debug.keystore 的文件，位置位于电脑的：`/Documents and Settings / 电脑用户名 /.Android/debug.keystore`。

## 我的应用能使用 debug 签名吗

如果您的应用是采用默认签名的方式（debug 签名），一旦换了新的签名应用将不能覆盖安装，必须将原先的程序卸载掉，才能安装上。因为程序覆盖安装主要检查两点：

1. 两个程序的入口 Activity 是否相同。两个程序如果包名不一样，即使其它所有代码完全一样，也不会被视为同一个程序的不同版本；
2. 两个程序所采用的签名是否相同。如果两个程序所采用的签名不同，即使包名相同，也不会被视为同一个程序的不同版本，不能覆盖安装。因此，使用 debug 签名存在以下风险：

1) debug 签名的应用程序不能在 Android Market 上架销售，它会强制您使用自己的签名；Debug 模式下签名用的证书（默认是 Eclipse/ADT 和 Ant 编译）自从它创建之日起，1 年后就会失效。

2) debug.keystore 在不同的机器上所生成的可能都不一样，就意味着如果您更换机器进行 Apk 版本升级，那么将会出现程序不能覆盖安装的问题。相当于软件不具备升级功能！

基于上述原因，我们不建议您使用 debug 签名作为应用的签名，除非您只是做本地测试。

## zipalign 优化

Zipalign 优化是对 Apk

文件进行存档对齐，确保所有的未压缩数据都从文件的开始位置以指定的对齐方式排列。尤其是. Apk 压缩包中的图片资源和未加工处理的相关文件，对齐的方式是以 4 字节对齐。

## zipalign 优化有什么好处

Zipalign 优化能够减少应用程序的 RAM 内存资源消耗。目前 Google Play 要求必须使用 zipalign 优化的安装包，其他应用市场暂无要求。

## 我是否需要选择 zipalign 优化

您可以结合实际情况来自选择是否 zipalign 优化。通常除上架 Google Play 外，无需做 zipalign 优化。

## 渠道包不成功

AndroidManifest.xml 文件属于二进制文件，若您使用文本编辑器（包括 notepad++、Editplus 等）打开会显示乱码。若您使用文本编辑器查看，可能找不到已成功写入的渠道名称，建议您使用 AXMLPrinter2 等软件查看。

## 什么是代码混淆

代码混淆通常将代码中的各种元素（变量、函数、类名等）改为无意义的名字，使得阅读的人无法通过名称猜测其用途，增大反编译者的理解难度。

虽然代码混淆可以提高反编译的门槛，但是对开发者本身也增大了调试除错的难度。开发人员通常需要保留原始未混淆代码用于调试。

## 代码混淆就安全了么

代码混淆并不能从根本上阻止反编译等。因为代码混淆仅仅提高了阅读难度，但并不能真正阻止反编译。因此，对于高安全要求的场景，代码混淆并不足够安全。

## 加固前需要代码混淆么

加固前不需要特意混淆，直接提交安装包进行加固即可。  
但是加固和代码混淆并不冲突。

## 加固和代码混淆的安全性比较

代码混淆仅提高了代码的阅读难度。

加固是多维度的安全防护方案，包括反破解、反逆向、防篡改等，可以防止应用被各类常见破解工具逆向，安全性要远大于单纯的代码混淆。

## 加固后无法安装

请确保您加固后已重新签名。

加固过程不可避免的会破坏签名，因此加固后的包需重签名，未签名应用将无法顺利安装。

## 加固后部分功能异常

通常是因为未（正确）签名导致。应用加固不会影响应用既有功能，请排查以下可能问题：

1. 应用加固前后签名不一致，或者未签名；
2. 应用本身有签名、文件 MD5 校验等校验机制；
3. 多次重复加固极易导致程序异常，请确保使用一次加固。推荐您上传原始安装包，使用应用安全进行加固。请勿用第三方加固包或应用安全加固包再次加固；

对于无法确认的问题，您可以联系我们。应用安全官方 QQ 群：218062986

## 加固失败：应用存在安全风险

说明应用被国内外杀毒引擎判定为恶意，应用安全将会拒绝对此类应用进行加固，请检查应用是否有违规行为！

应用安全采信了第三方杀毒引擎判定结果。若您的应用被杀毒引擎判定为恶意，是否加固已经无意义，因该类应用将无法上架正规应用市场，无法安装到用户手机，也注定会被手机的安全防护软件拦截。此类问题非加固造成，还请仔细检查应用是否违规。

## 加固失败：重新加固

通常因超时等不可控因素，建议您点击重新加固。

若多次仍不能解决，请联系我们：应用安全官方 QQ 群 218062986

## 加固步骤

您只需要确保使用 已签名 的安装包在应用安全直接提交加固即可。

## 加固须知

另外，因加固过程不可避免的会破坏签名，请务必在加固后重签名。签名后的加固包发布到各应用市场即可。

## 上传失败的原因有哪些？

1. 上传的应用未签名
2. 目前应用安全仅允许上传已签名应用。
3. 应用存在安全风险

若第三方杀毒引擎提示您的应用存在安全风险，则应用安全会拒绝您的上传、拒绝对应用进行加固。一旦出现该情形，建议您检查应用中是否存在违规行为。

若您将该应用发布出去，极大可能被渠道市场拒绝、无法在用户手机安装。对于此类应用，加固能否成功并非最核心要素，因为渠道分发、用户手机都会有类似的安全扫描，应用安全采信的第三方杀毒引擎也极有可能被各分发市场、用户手机上安装的安全软件采信。

该类应用正真的问题在于，很难发布到正规市场、安装到用户手机上去，而非无法加固。

4. 部分浏览器可能存在不兼容情况，推荐使用最新的 chrome、IE 浏览器或 QQ 浏览器。

## 加固为什么必须重签名

应用加固不可避免的会破坏原有签名，加固后必须对加固包重签名才能发布至应用市场，否则会被提示“应用未签名”。请务必确保加固前后的签名一致。

## 为什么签名失败

签名失败的原因通常有以下情况：

1. 密码错误
2. 签名文件错误
3. 加固包下载不正确：请您检查下加固包体积是否过小。因网络原因，若您的包下载时间过久，可能还未下载完成已经被浏览器强制置为完成，导致下载的加固包实际是残缺的。
4. 权限不足：受限用户自身系统、环境权限设定。签名工具可能无读写签名文件路径的权限。建议您可以把签名文件放在签名工具目录下重试。  
若您确认无以上问题，仍然签名失败，可以联系我们。应用安全官方 QQ 群：218062986

## 签名工具中的签名信息（keystore 路径、keystore 密码、keystore 别名）

签名信息请向您的开发人员索取，签名文件一般为 keystore 或 jks 的扩展名文件。

## 上传应用后提示缺少标签

Apk 中的 androidmanifest.xml 文件描述了应用的基本信息。

标签属性是一个重要的基础信息，应用安全平台对 Apk 文件中的 androidmanifest.xml 文件解析后，会获取其中的 Application 和 activity 节点下的 android:label 字段的值，并作为 Apk 的标签信息保存。如果该字段为空，应用安全会提示“Apk 缺少标签”。

若您上传时提示 Apk 缺少标签，建议您按照标准填写 androidmanifest.xml 文件的 android:label 字段。

## 兼容性测试

### 为什么要做兼容性测试？

Android 机型、系统碎片化严重，每一款应用在上架之前，都应做一轮覆盖一定机型量的兼容性测试。

在产品面对海量用户之前，尽量筛选出并解决所有影响用户体验的问题。

我们大致将主要问题分为以下 8 种：

### 如何进行测试机型选择？

理论上机型数量覆盖越多，可发现的 Bug 越多。

然而，“最需要修复的 Bug 80% 都集中在了 20% 的机器上”，80/20 原则在适配兼容测试过程中也同样适用。大量的测试机器中必然充斥着众多边缘机型；这些机型所测出的兼容性问题，不仅修改成本高，而且修复后产生的作用也并不显著，开发拿到了一堆测试提交的冷僻机型上的 BUG，不免有鸡肋之感：修之无味，弃之可惜。

建议花更多的时间在最主流机型的主要 Bug 上，以腾讯游戏项目为例，测试 TOP100 的机型。机型排名根据腾讯游戏大数据平台选取，确保用户量占比最高。每月进行新机型采购，保持机型库中的 TOP100 机型全都是当下的最热机型。

而作为移动安全兼容性测试的用户，均享受与腾讯应用同等的兼容性测试服务。

## 安全测评

### 安全测评能解决什么问题？

虽然通过应用加固，可以对 APP 程序进行整体的保护。但对于 APP 的编程代码、第三方控件、以及残留信息等方面，是否存在代码风险，已知漏洞，是否存在后门等恶意代码，是否存在违法违规，暴露自身运行逻辑的敏感信息，就需要进行全面的安全测评，发现潜在的应用安全问题。

### 腾讯云应用安全检测能力如何？

腾讯云安全测评，包括代码风险、漏洞扫描、第三方 SDK 检测、恶意代码扫描，以及敏感词检测等全方面的安全测评能力。并且，基于腾讯的全网终端覆盖，对于新风险、新威胁，能够第一时间反馈至应用安全测评能力，并转化为腾讯云用户的价值。

### 安全测评发现的问题，应该怎么办？

1. 安全测评报告中，不仅会提供直观的测评结果，同时会将问题的具体位置、相关代码反馈用户，使用户能够快速定位到问题。
2. 针对每一项测评结果中发现的问题，均配以相应的解决建议，建议具体到配置某个参数、代码，从而帮助用户快速解决问题。

### 应用在什么阶段进行安全测评？

1. 建议用户在开发阶段中，可根据需要进行安全测评，及时发现并解决问题；
2. 在应用发布前的测试阶段，建议进行安全测评，确保待发布应用的安全性；

### 使用未加固安装包，还是已加固安装包进行安全测评？

因为加固后部分代码已加密加壳，建议用户使用未加固安装包进行检测，能够更深度的发现潜在的风险和漏洞。

### 敏感词检测是什么，有什么用？

由于敏感词导致的潜在风险：

1. 若应用中存在涉黄、涉暴恐等违法违规的文字信息，不仅会影响开发者自身品牌，很可能会直接面临法律法规风险，承担相关责任。
2. 若开发测试过程中，代码说明，调试信息，以及一些测试用的账户密码等信息残留，对于应用自身的安全风险无疑是极大的。

腾讯云敏感词检测，基于预置的敏感词库，能够有效帮助用户规避安全隐患；并且，用户可以通过腾讯云控制台，自行配置敏感词用于安全测评。

## 安全软键盘

### 使用 Android 系统默认软键盘有什么风险？

应用程序中的敏感信息，通常主要来源于使用者的直接输入，如果用户的输入数据被监听或者按键位置被记录，很可能导致用户的输入数据被获取，从而使账号、密码等隐私信息泄露。而 Android 系统的默认输入键盘对上述风险并未进行有效保护。

### 腾讯云安全软键盘有什么能力？

1. 软键盘随机键位，防止按键位置记录；
2. 输入信息不回显，防止截屏攻击；
3. 输入数据全加密，即使在内存中也是以加密形态存在，防止输入数据被监听；

### 如何使用安全软键盘？

腾讯云安全软键盘为收费安全组件，以 SDK 的形式进行集成即可。

## 崩溃检测

### 如何使用崩溃监测？

1. 在腾讯云移动安全控制台，开通崩溃监测服务；
2. 注册产品，完善开发者信息；
3. 按提示下载并集成崩溃监测 SDK；
4. 实时查看崩溃监测数据，及时发现问题；

### 崩溃监测可以监测哪些事件？

应用崩溃事件、ANR 事件，以及用户自定义的错误事件，均能够全面监测。

### 崩溃监测服务收费吗？

腾讯云移动安全用户，可免费使用崩溃监测服务。

## 白盒密匙

### 什么是白盒密钥？

现在的 APP 针对账户信息、密码等重要数据，往往使用加密算法进行加密保护。但是对于加密算法，其可靠性的核心在于加密密钥的安全，腾讯云白盒密钥基于白盒密码技术，能够有效保护加密密钥的安全；

### 支持哪些加密算法？

支持 DES、3DES、AES、SM4 等加密算法；

### 如何使用白盒密钥？

腾讯云白盒密钥为收费安全组件，以 SDK 形式集成使用；

使用时，仅需用原始密钥对白盒密钥 SDK 进行初始化。后续在应用中，直接调用白盒密钥 SDK 即可完成加解密操作，而不会再以任何形式存在原始密钥。

## 盗版监控

### 盗版应用有什么危害？

对于盗版应用，有但不限于如下情况：

1. 存在恶意代码的钓鱼应用，盗取用户重要信息；
2. 直接窃取正版代码二次打包后发布的盗版应用，利用他人成果牟利；
3. 植入广告或下载链接，影响正版应用用户量；
4. 破解应用中的收费功能，造成应用的收益下降。

无论何种方式，都将对应用的合法开发者造成品牌及经济收益的损害。

### 盗版监控是如何判断盗版软件的？

主要是根据应用名称、应用安装包名，以及应用的签名证书等多个维度综合分析判定。

### 盗版监控服务收费吗？

盗版监控服务分为免费版本和收费版本，主要是在盗版监控覆盖范围有所区分；另外，收费版本在盗版的打击能力方面，不仅包括渠道下架，还将提供盗版传播、运行等方面的实时打击能力。

具体请联系腾讯云移动安全咨询。

### 如何使用腾讯云盗版监控服务？

1. 在腾讯云移动安全控制台，开通盗版监控服务；
2. 用户上传正版应用的安装包；
3. 腾讯云移动安全进行应用正版验证，及应用所有权验证；
4. 线上查看应用盗版监控的统计分析数据；

### 腾讯云盗版监控有什么优势？

覆盖 12 亿移动终端，数据的准确性、真实性，以及全网覆盖程度等各方面能力，具有绝对优势