

## 什么是包名？

每个 Android 应用均有一个唯一的应用 ID。安卓以 Java 包的形式管理应用。具体说明见官方文档：

```
android {  
    defaultConfig {  
        applicationId "com.example.myapp" ← 应用包名  
        minSdkVersion 15  
        targetSdkVersion 24  
        versionCode 1  
        versionName "1.0"  
    }  
    ...  
}
```

<https://developer.android.com/studio/build/application-id.html>

## 什么是签名文件？

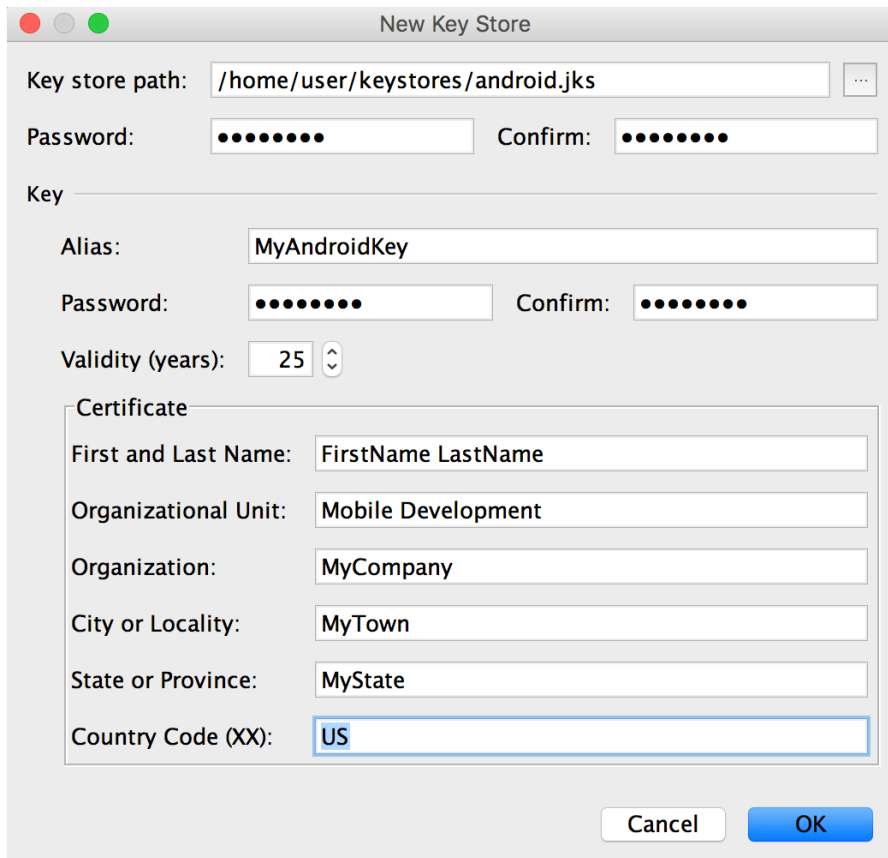
安卓 apk 需要开发者进行签名。开发调试过程中，IDE(android studio,Eclipse) 会使用默认的 debug 签名文件进行签名。但发布 apk 时必须使用，自己生成的签名文件进行签名。签名文件确保了开发者对该应用的所有权，因为不同签名文件签名的 apk 不能覆盖原有的。该文件扩展名为 jks。

## 如何生成新的签名文件

您可以使用 Android Studio 生成应用签名或上传密钥，步骤如下：

1. 在菜单栏中，点击 Build > Generate Signed APK。
2. 从下拉菜单中选择一个模块，然后点击 Next。
3. 点击 Create new 以创建一个新密钥和密钥库。

4. 在 New Key Store 窗口上，为您的密钥库和密钥提供以下信息，如图 3 所示。



The screenshot shows the 'New Key Store' dialog box. It has a title bar with red, yellow, and green window control buttons. The main content area includes the following fields and sections:

- Key store path:** A text field containing '/home/user/keystores/android.jks' and a file browser button (three dots).
- Password:** A text field with masked characters (dots) and a 'Confirm:' field with masked characters.
- Key:** A section containing:
  - Alias:** A text field containing 'MyAndroidKey'.
  - Password:** A text field with masked characters and a 'Confirm:' field with masked characters.
  - Validity (years):** A text field containing '25' and a small dropdown arrow.
- Certificate:** A section containing several text fields:
  - First and Last Name:** Contains 'FirstName LastName'.
  - Organizational Unit:** Contains 'Mobile Development'.
  - Organization:** Contains 'MyCompany'.
  - City or Locality:** Contains 'MyTown'.
  - State or Province:** Contains 'MyState'.
  - Country Code (XX):** Contains 'US'.
- Buttons:** 'Cancel' and 'OK' buttons at the bottom right.

### 密钥库

- Key store path: 选择创建密钥库的位置。
- Password: 为您的密钥库创建并确认一个安全的密码。

### 密钥

- Alias: 为您的密钥输入一个标识名。
- Password: 为您的密钥创建并确认一个安全的密码。此密码应当与您为密钥库选择的密码不同
- Validity (years): 以年为单位设置密钥的有效时长。密钥的有效期应至少为 25 年，以便您可以在应用的整个生命期内使用相同的密钥签署应用更新。
- Certificate: 为证书输入一些关于您自己的信息。此信息不会显示在应用中，但会作为 APK 的一部分包含在您的证书中。

填写完表单后，请点击 OK。

具体说明见官方文档：

<https://developer.android.com/studio/publish/app-signing.html>

## 什么是签名 MD5? 如何获取

每个签名文件都有一个数字指纹。相当于是公钥，同一个签名文件的指纹是一样的，不同的签名文件指纹不一样。可以通过检查这个指纹确定是不是使用的同一个签名文件。百度人脸鉴权服务使用的是 MD5 方式的指纹。

命令行输入 `keytool -list -v -keystore <签名文件路径>`

然后输入密码，会打印出该签名文件相关的信息。其中的一项是证书指纹 MD5

```
Desktop keytool -list -v -keystore keystore.jks
输入密钥库口令:
[
  密钥库类型: JKS
  密钥库提供方: SUN

  您的密钥库包含 1 个条目

  别名: key0
  创建日期: 2017-9-22
  条目类型: PrivateKeyEntry
  证书链长度: 1
  证书 [1]:
  所有者: CN=test
  发布者: CN=test
  序列号: 631d534b
  有效期开始日期: Fri Sep 22 11:29:45 CST 2017, 截止日期: Tue Sep 16 11:29:45 CST 2042
  证书指纹:
    MD5: 7D:CC:67:D9:01:42:1F:6C:0A:6B:50:D0:EF:4E:52:E9      MD5值
    SHA1: 29:94:AD:64:7A:20:3A:CD:68:BF:7D:AD:D7:10:F5:75:56:E6:9C:F7
    SHA256: CD:1A:7B:02:36:FF:8C:A9:48:C6:07:39:B9:17:7F:5D:C4:49:7E:75:E0:77:04:C3:B5:E7:AA:64:3F:A2:EF:3
    签名算法名称: SHA256withRSA
    版本: 3
]
```

## 为什么需要签名 MD5?

安卓的应用是以包名做为唯一 ID 的。百度的人脸服务也是以包名做为单位进行授权的。因为包名是开发者填写的，所以别的开发者也可以写个应用来冒充其他人的应用。百度人脸服务会涉及到用户的信息，使用过程中也有费用产生。所以为了保护 app 不会他人冒充，我们对应用的签名进行校验。刚才也提到了，因为 MD5 算法的不可逆性，可以当做公钥使用。用户在申请时在后台填写签名的

MD5 值，发布/测试时，使用该签名文件。人脸服务在运行时会对当前应用的签名 MD5 进行校验，如果信息不一致会拒绝服务。