

android签名机制

Last edited by **caoquanli** 1 month ago

android签名机制

——了解签名

1.为什么要签名？ 如果不签名呢？

为了防止APP反编译替换原有的程序，如果有相同包名的应用存在，新的APk则不能安装在设备上。就算被反编译，在没有原有私钥的情况，重新签名生成的apk和原来的apk的标志是不同的。如此，被修改的apk如果安装在原来的设备上，则会提示：

Failure [INSTALL_PARSE_FAILED_NO_CERTIFICATES]

如果不签名，直接安装到设备上会提示:

 **fail** 在android源码目录build\target\product\security 有好几种签名密钥：

- **media.pk8与media.x509.pem**
- **platform.pk8与platform.x509.pem;**
- **shared.pk8与shared.x509.pem;**
- **testkey.pk8与testkey.x509.pem;**

其中 *.**pk8** 文件为私钥， *.**x509.pem** 文件为公钥,采用的加密方式是非对称加密，因此上面有四个密钥对，分别是media, paltform, shared, testkey。

在apk的android.mk文件中会指定LOCAL_CERTIFICATE 变量：

```
# 普通APK，默认情况下使用
LOCAL_CERTIFICATE := testkey
# 该APK完成一些系统的核心功能。
LOCAL_CERTIFICATE := platform
# 该APK需要和home/contacts进程共享数据
LOCAL_CERTIFICATE := shared
# 该APK是media/download系统中的一环
LOCAL_CERTIFICATE := media
```

系统中所有使用android.uid.system作为共享UID的APK 都应该使用platform签名，AndroidManifest里面必须添加 android:sharedUserId="android.uid.system"才有用，可以参见Settings应用。如果没有指定LOCAL_CERTIFICATE变量就使用默认签名。

——制作release版系统签名

在制作签名之前,我们需要先生成密钥。要生成您自己的唯一发布密钥集，请在Android的根目录下运行以下命令：

```
subject='/C=CN/ST=Shang Hai/L=Huang Pu/O=Suntec/OU=FrameWork/CN=sunchao/emailAddress=androi
mkdir ~/.android-certs
for x in releasekey platform shared media; do \
    ./development/tools/make_key ~/.android-certs/$x "$subject"; \
done
```

其中subject要修改为你自己的信息,创建的.android-certs文件集也可以根据自己的要求修改。

- C=CN 国家的名字*
- ST=Shang Hai 省的名字*
- L=Huang pu 市的名字*
- O=Suntec 公司的名字*
- OU=FrameWork 部门名字*
- CN=sunchao 制作者名字*

执行命令后，会让你设置密码，一直回车键。会在文件夹.android-certs文件夹里面生成四个密钥对，复制四个密钥对到build\target\product\security目录下面，并覆盖掉里面原来的密钥对。 根据自己的平台在/device/mediatek/mt2712下面修改device.mk 里面添加属性：
PRODUCT_DEFAULT_DEV_CERTIFICATE := build/target/product/security/releasekey

并且修改目录build/core下面的MakeFile文件，修改为：

```
#ifeq ($(DEFAULT_SYSTEM_DEV_CERTIFICATE),build/target/product/security/testkey)
#BUILD_KEYS := test-keys
ifeq ($(DEFAULT_SYSTEM_DEV_CERTIFICATE),build/target/product/security/releasekey)
BUILD_KEYS := release-keys
```

编译整个系统。此时编译出来的版本release版。

直接给应用签名

直接签名还需要一个signapk.jar文件，此文件位置在out/host/linux-x86/framework/signapk.jar 在利用上面文件签名
eg：给APK使用platform签名 命令：

```
java -jar signapk.jar platform.x509.pem platform.pk8 app.apk app_signed.apk
```

app_signed.apk为经过系统签名的apkl。