软证书申请指导

采用OpenHarmony系统的设备，在固件开发中的功能调测、生产试制、产品量产过程，均需要使用设备授权证书。本章节指导伙伴为OpenHarmony设备申请对应的授权证书。当前只支持设备软证书（以下代称“软证书”）。软证书具有唯一性：一台设备只能预置一个软证书，一个软证书也只能对应一台设备。

说明

· 为了提高生产效率，伙伴应当在固件设计和实现时预留软证书读写接口，以便在设备生产时批量写入软证书。

· 在"设备管理"->"管理软证书"中，可以下载manuKey.key文件。在产品集成开发（详细参见"设备管理"->"管理软证书"中SDK包内容）时，需要将这秘钥写入固件代码中对应的OEMGetManufactureKey接口，以便固件能够正确处理软证书。

软证书生成机制

由于软证书对于设备非常重要，平台采用了非对称加密传输的方式管理软证书，以确保只有持有私钥的申请人员才能解密软证书文件。整体流程如下：

1. 伙伴在本地生成私钥和公钥文件。
2. 申请软证书时，平台需要伙伴提供公钥。
3. 平台根据申请额数量，生成一批软证书。为了方便处理，平台会把这一批软证书包装为一个txt文件。同时为了提高传输效率，平台还会对txt文件进行压缩生成zip文件。
4. 平台最后根据伙伴上传的公钥对zip文件进行加密，生成以“.lic”为后缀名的加密文件，并在平台上提供链接给伙伴下载。
5. 伙伴下载lic文件后，使用自己本地保存的私钥文件解密出zip文件。最后通过解压zip文件得到txt文件，即可从txt文件中逐一获取到设备软证书。

准备工作

在申请软证书前，需要基于RSA算法生成**私钥**和**公钥。**公钥需要在申请软证书时提供给平台，用于平台加密软证书文件；私钥用于伙伴解密申请到的软证书文件。

1. 准备一台安装有**OpenSSL**的PC。Linux系统的PC通常自带OpenSSL，推荐使用。
2. 在命令行窗口中，执行如下命令，生成私钥。

   ```
   openssl genrsa -out rsa_private_key.pem 1024
   ```

   ```
   openssl pkcs8 -topk8 -inform PEM -in rsa_private_key.pem -outform PEM -nocrypt >> privatekey.txt
   ```

命令执行成功后，得到“rsa_private_key.pem”（标准格式）和“privatekey.txt”（pkcs8格式）两个私钥文件。前者用于生成公钥文件；后者用于解密软证书文件。

3. 继续执行如下命令，生成私钥对应的公钥。

   ```
   openssl rsa -in rsa_private_key.pem -pubout -out rsa_public_key.pem
   ```

命令执行成功后，得到“rsa_public_key.pem”文件。用文件编辑器打开该文件，拷贝公钥信息（不要拷贝第一行和最后一行，即“BEGIN PUBLIC KEY”、“END PUBLIC KEY”所在的两行信息），以备后续获取软证书使用。

注意

· 私钥是解密软证书文件的唯一凭证，伙伴生成私钥文件后务必妥善保存。私钥丢失将无法解密lic文件，私钥泄露将面临软证书被盗用的风险。

· 私钥与公钥的生成只需要执行一次，后续在申请软证书的过程中可以重复使用。

获取软证书

软证书作为设备凭据，需要依据实际设备数量为产品申请软证书或提升额度。

实际操作请参考兼容性平台-设备管理-管理软证书板块。

说明

· 软证书的剩余额度= 总额度-已申请。伙伴通过实名兼容性测评后，将获得默认分配的500个软证书额度。

· 申请记录提供7天内软证书的下载，请及时下载并妥善保管软证书。

· 软证书本身并无有效期限制。在私钥未被泄露的条件下，软证书可以一直正常使用。

· 如果申请状态为“失败”，根据报错信息，处理后重新提交申请。

解密软证书

准备JAVA运行环境JRE。

为保证解密工具的正常运行，需要在本地PC上搭建JAVA运行环境JRE，并配置环境变量。如果已经满足环境要求，可跳过该步骤。

步骤1：下载JRE并进行安装。

步骤2：配置JAVA环境变量，具体操作可自行查阅相关资料（查询关键词：JRE的安装及环境变量配置）。

获取解密工具。

. 实际操作请参考兼容性平台-设备管理-管理软证书板块。

解压“解密工具.zip”文件，得到“RsaDec.bat”和“RsaDec_x.x.x.jar”两个文件，将他们与被加密软证书放在同一个文件夹下。

说明

建议将解密工具解压到独立文件夹，并在该文件夹下再新建子文件夹，分别用于管理不同时间申请到的加密软证书。

运行解密工具，完成软证书解密。

. 双击“RsaDec.bat”文件，快速完成解密。

说明

. 默认情况下“RsaDec.bat”不会对已解密的文件再次进行解密，可以重复运行该工具。

. 除了直接运行解密工具，也可以通过命令行执行解密工具，具体执行方式可参考配套的工具说明。

. 对解密完成后生成的同名zip文件进行解压，即可获得软证书。

解压`XXX.zip`，生成`.txt`文件，即可从中获取到产品软证书。

说明

. 默认使用`*.lic`文件所在路径下的私钥去解压。如果文件夹下不存在私钥文件，则以父文件夹下对应的私钥文件为准。

. 暂不支持文件路径以及文件名中包含`!`、`^`字符。