

AG35-QuecOpen

SecBoot 应用指导

LTE 系列

版本：AG35-QuecOpen_SecBoot_应用指导_V1.0

日期：2017-12-02

状态：临时文件



上海移远通信技术股份有限公司始终以为客户提供最及时、最全面的服务为宗旨。如需任何帮助，请随时联系我司上海总部，联系方式如下：

上海移远通信技术股份有限公司
上海市徐汇区虹梅路 1801 号宏业大厦 7 楼 邮编：200233
电话：+86 21 51086236 邮箱：info@quectel.com

或联系我司当地办事处，详情请登录：

<http://quectel.com/cn/support/sales.htm>

如需技术支持或反馈我司技术文档中的问题，可随时登陆如下网址：

<http://quectel.com/cn/support/technical.htm>

或发送邮件至：support@quectel.com

前言

上海移远通信技术股份有限公司提供该文档内容用以支持其客户的产品设计。客户须按照文档中提供的规范、参数来设计其产品。由于客户操作不当而造成的人身伤害或财产损失，本公司不承担任何责任。在未声明前，上海移远通信技术股份有限公司有权对该文档进行更新。

版权申明

本文档版权属于上海移远通信技术股份有限公司，任何人未经我司允许而复制转载该文档将承担法律责任。

版权所有 ©上海移远通信技术股份有限公司 2018，保留一切权利。

Copyright © Quectel Wireless Solutions Co., Ltd. 2018.

文档历史

修订记录

版本	日期	作者	变更表述
1.0	2018-12-22	钱润生	初始版本

目录

文档历史	2
目录	3
表格索引	4
图片索引	5
1 启动安全	6
1.1. 启动流程	6
1.2. SECBOOT 能够校验的文件	7
2 证书链制作	8
2.1. 环境准备	8
2.2. 生成证书	8
2.3. 替换证书	9
3 镜像签名	10
3.1. 基于 SECBOOT 的 IMG 签名	10
3.2. HLOS 的 kernel 签名	12
3.2.1. 根证书添加到 aboot 代码里	12
3.2.2. 签名 kernel img	13
4 安全烧录	14

表格索引

图片索引

图 1 安全启动流程.....	6
-----------------	---

1 启动安全

1.1. 启动流程

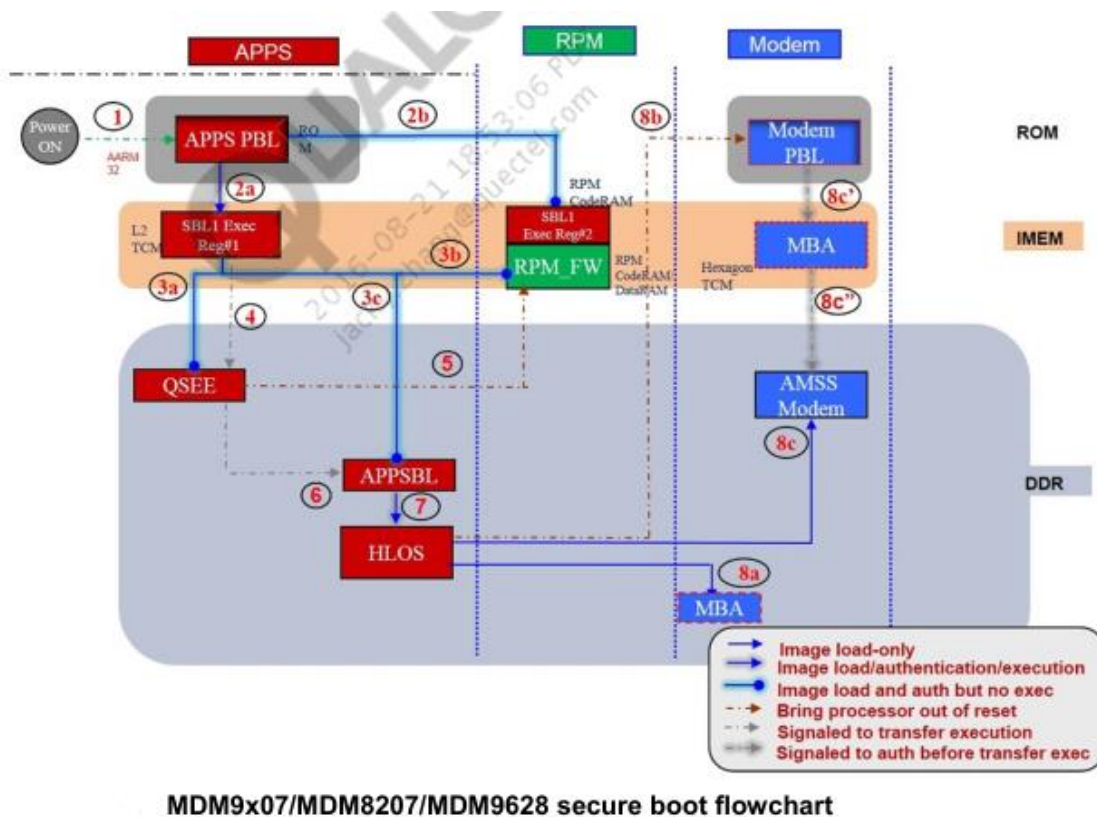
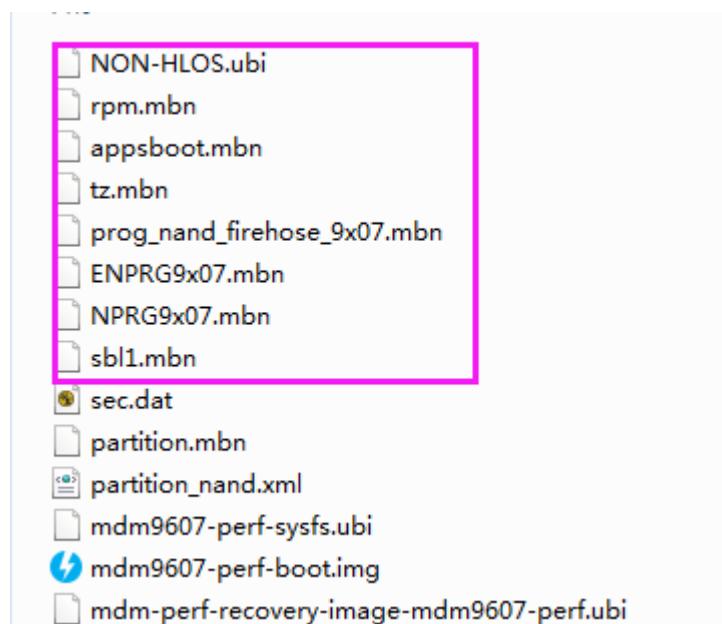


图 1 安全启动流程

AG35 的安全启动按照对 img 的签名格式分为三大部分：

- (1) 高通传统的 secboot 机制，本部分不能对 HLOS (kernel+FS) 两个 img 文件签名。
- (2) Kernel 的鉴权，本部使用有公钥的证书在 aboot 文件里
- (3) Linux 文件系统的鉴权，本部分基于 DM-VERITY 实现

1.2. SECBOOT 能够校验的文件

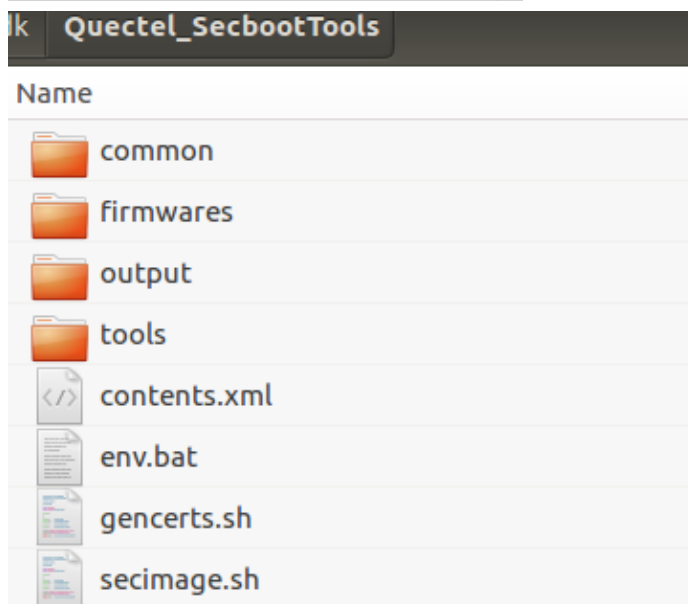


2 证书链制作

2.1. 环境准备

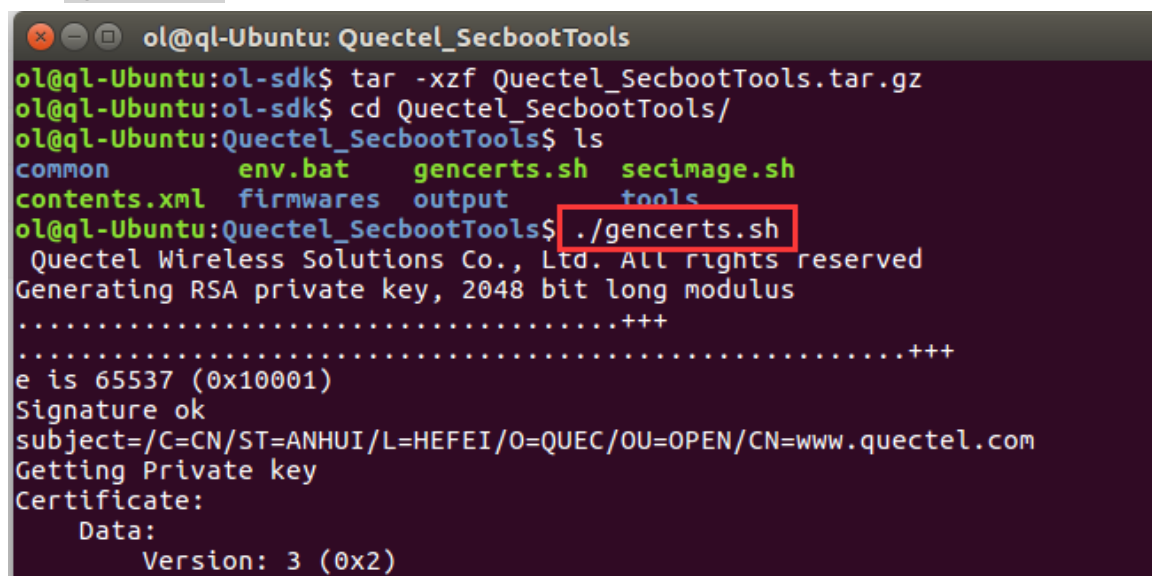
- (1) 环境: ubuntu, Python2.7, openssl 版本 1.0.2 以上
- (2) 获取工具包 Quectel_SecbootTools.tar.gz, 执行

```
tar -xzf Quectel_SecbootTools.tar.gz
```

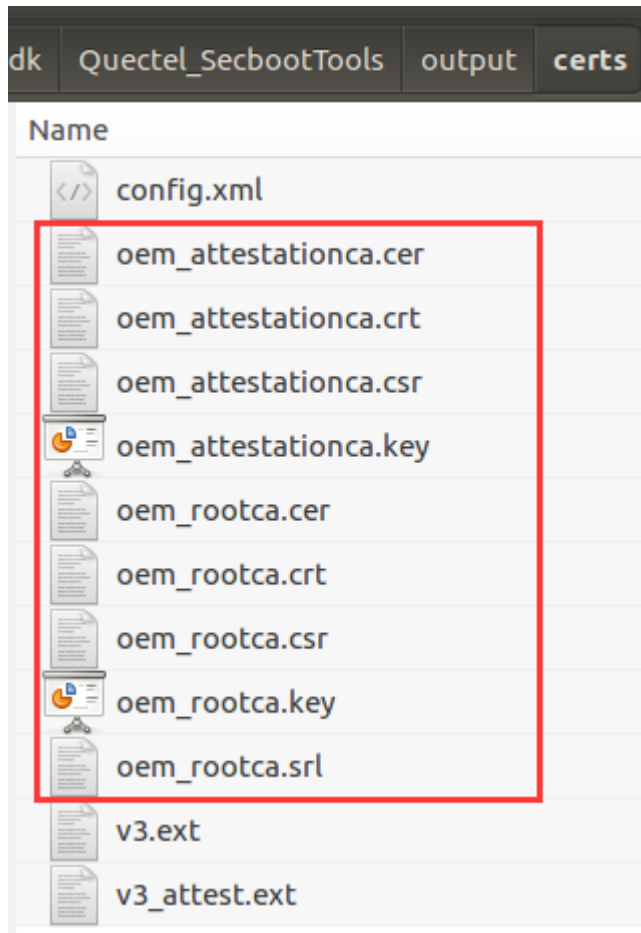


2.2. 生成证书

执行 ./gencerts.sh



生成的证书链在 output/certs, 如图所示



2.3. 替换证书

把新生成的 **oem_rootca.key** **oem_rootca.cer** **oem_attestationca.key** **oem_attestationca.cer** 四个文件拷到 `common/sectools/resources/data_prov_assets/Signing/Local/quectel_certs-key2048_exp65537`

3 镜像签名

3.1. 基于 SECBOOT 的 IMG 签名

(1) 获取最新的固件包

将最新的固件包解压，把工具包 [Quectel_SecbootTools/firmwares](#) 文件下所有文件替换。具体文件内容如下：

```
ol@ql-Ubuntu:firmwares$ tree
.
├── appsboot.mbn
├── ENPRG9x07.mbn
├── modem
│   └── 9607.genns.prod
│       ├── efs1.bin
│       ├── efs2.bin
│       ├── efs3.bin
│       ├── efs_image_meta.bin
│       ├── mba.mbn
│       ├── mcfg_hw.mbn
│       ├── mcfg_sw.mbn
│       ├── non-reloc
│       │   ├── qdsp6sw.mbn
│       │   └── unsigned
│       │       └── qdsp6sw.mbn
│       ├── qdsp6sw.mbn
│       ├── unsigned
│       │   ├── mba.mbn
│       │   └── qdsp6sw.mbn
├── NPRG9x07.mbn
├── prog_nand_firehose_9x07.mbn
├── sbl1.mbn
└── tz.mbn
```

(2) fuse 配置

在 common\sectools\config\9607 目录下，打开 9607_fuseblower_USER.xml 文件

```

9607 fuseblower_USER.xml
</metadata>
<secdat>
  <file_info>default dat file</file_info>
  <file_version>1</file_version>
  <fuse_version>1</fuse_version>
</secdat>
<module id="SECURITY_CONTROL_CORE">
  <entry ignore="false">
    <description>contains the OEM public key hash as set by OEM</description>
    <name>root cert hash</name>
    <value>83729ec586e3693c2115d83c675868bbcf470d9feb968ce198cb0437d485b2f2</value>
  </entry>
  <entry ignore="true">
  <entry ignore="false">
    <description>PK Hash is in Fuse for SEC BOOT1 : Apps</description>
    <name>SEC_BOOT1_PK_Hash_in_Fuse</name>
    <value>true</value>
  </entry>
  <entry ignore="false">
  <entry ignore="false">
  <entry ignore="false">
    <description>PK Hash is in Fuse for SEC BOOT2 : MBA</description>
    <name>SEC_BOOT2_PK_Hash_in_Fuse</name>
    <value>true</value>
  </entry>
  <entry ignore="false">
  <entry ignore="false">
  <entry ignore="false">
    <description>PK Hash is in Fuse for SEC BOOT3 : MPSS</description>
    <name>SEC_BOOT3_PK_Hash_in_Fuse</name>
    <value>true</value>
  </entry>
</module>

```

(3) 设备配置

在 common\sectools\config\9607 目录下，打开 9607_secimage.xml 文件，

```

9607_secimage.xml
See documentation on general_properties below.
-->
<general_properties>
  <selected_signer>local</selected_signer>
  <selected_encryptor></selected_encryptor>
  <selected_cert_config>quectel_certs</selected_cert_config>
  <ass_capability>secboot_sha2_root</ass_capability>

  <key_size>2048</key_size>
  <exponent>65537</exponent>

  <mrc_index>0</mrc_index>
  <num_root_certs>1</num_root_certs>

  <!-- MDM9207: 0x000480E1 -->
  <!-- MDM9607: 0x0004A0E1 -->
  <!-- MDM9628: 0x0004B0E1 -->
  <msm_part>0x0004A0E1</msm_part>
  <oem_id>0x0000</oem_id>
  <model_id>0x0000</model_id>
  <debug>0x0000000000000002</debug>

  <max_cert_size>2048</max_cert_size>
  <num_certs_in_certchain>3</num_certs_in_certchain>
</general_properties>

```

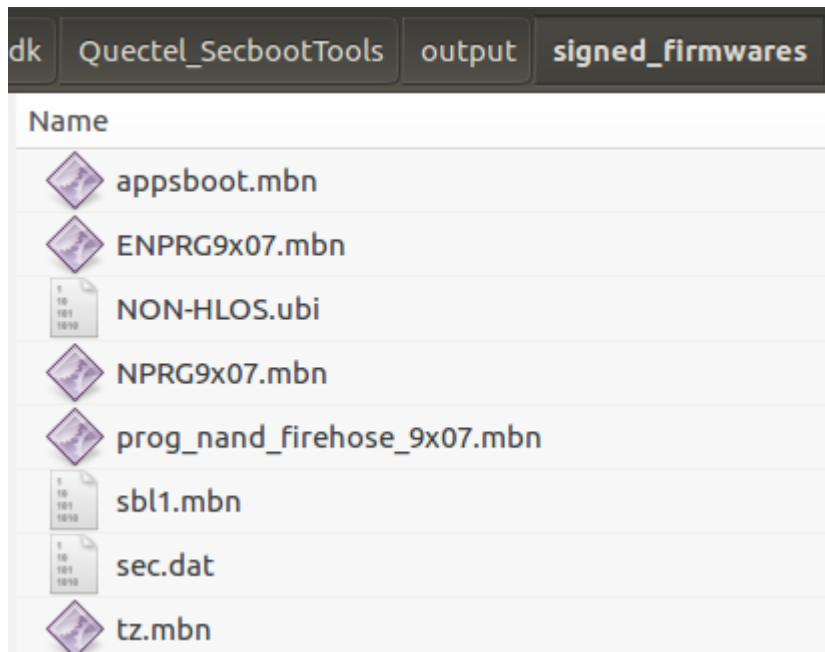
(4) 签名所有 img

在 **Quectel_SecbootTools** 工具包目录下，运行 secimage.sh 脚本

```
ol@ql-Ubuntu:firmwares$ cd ..
ol@ql-Ubuntu:Quectel_SecbootTools$ ./secimage.sh
Quectel Wireless Solutions Co., Ltd. All rights reserved
Gen sec.dat...
Logging to /home/ol/ol-sdk/Quectel_SecbootTools/output/fuseblower_output/FuseBlower_log.txt
```

(5) 获取签名镜像

在 Quectel_SecbootTools/output/signed_firmwares 文件下可获取签过名的 img



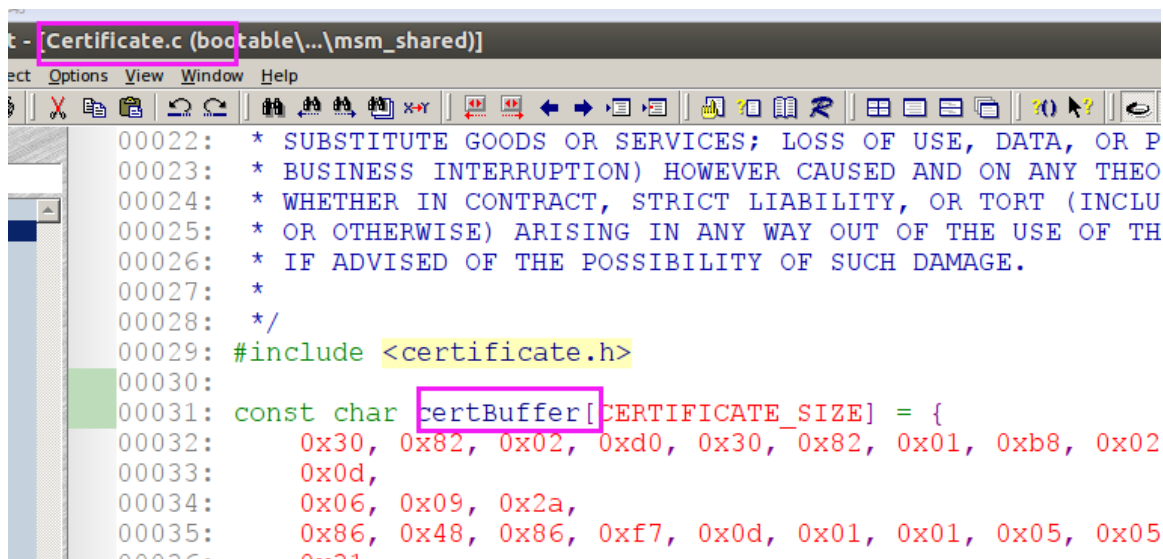
3.2. HLOS 的 kernel 签名

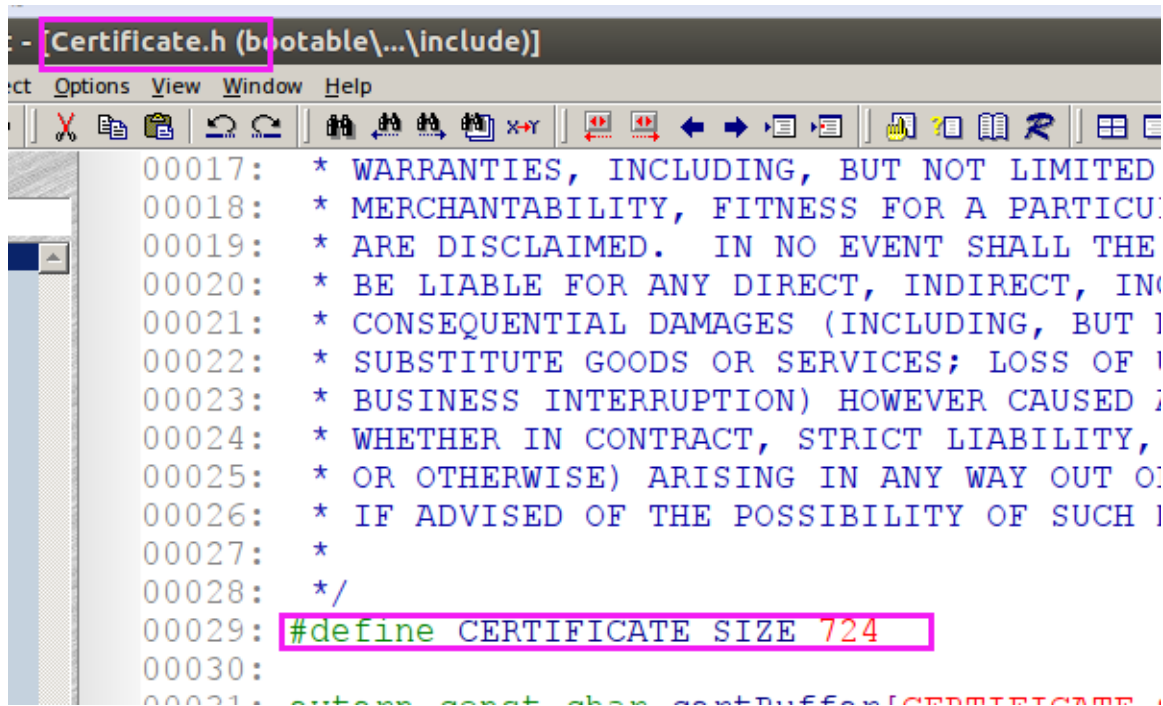
3.2.1. 根证书添加到 about 代码里

注意这一步做完了，需要重新签名 about

`xxd -i oem_rootca.cer`

替换 certificate.c 文件里面数组的 certBuffer 数组内容和 certificate.h 文件里面数组宏大小





```

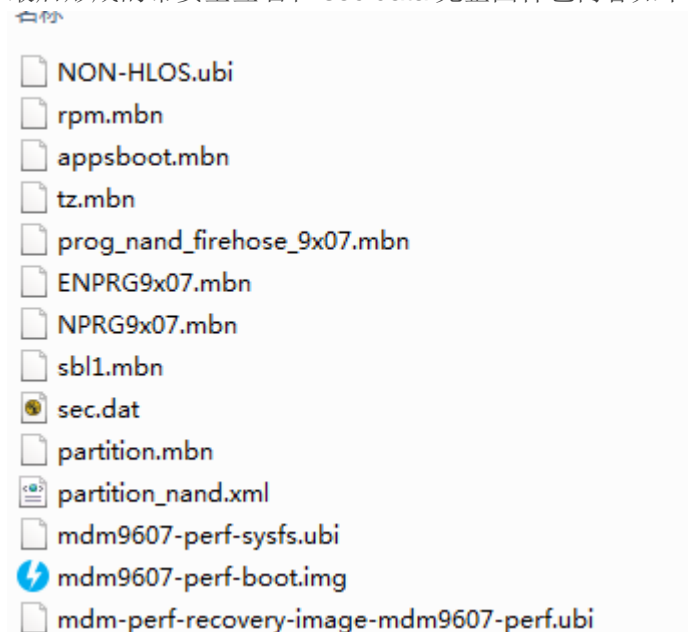
Certificate.h (bootable\...\include)
Options View Window Help
00017:  * WARRANTIES, INCLUDING, BUT NOT LIMITED
00018:  * MERCHANTABILITY, FITNESS FOR A PARTICULAR
00019:  * ARE DISCLAIMED.  IN NO EVENT SHALL THE
00020:  * BE LIABLE FOR ANY DIRECT, INDIRECT, IN
00021:  * CONSEQUENTIAL DAMAGES (INCLUDING, BUT
00022:  * SUBSTITUTE GOODS OR SERVICES; LOSS OF
00023:  * BUSINESS INTERRUPTION) HOWEVER CAUSED
00024:  * WHETHER IN CONTRACT, STRICT LIABILITY,
00025:  * OR OTHERWISE) ARISING IN ANY WAY OUT OF
00026:  * IF ADVISED OF THE POSSIBILITY OF SUCH
00027:  *
00028:  */
00029:  #define CERTIFICATE_SIZE 724
00030:
00031:  extern const char certBuf[CERTIFICATE_SIZE];
    
```

3.2.2. 签名 kernel img

- (1) 替换 ql-ol-extsdk/tools/quectel_mkboot/quectel.key 私钥。
- (2) 重新制作内核镜像，参照《Quectel_EC2x&AG35-QuecOpen_快速入门》

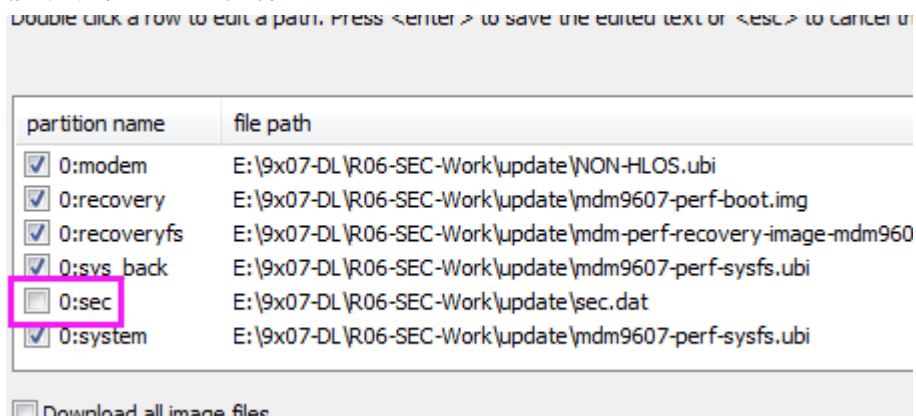
4 安全烧录

最后形成的带安全签名和 sec.data 完整固件包内容如下：



其中 **sec.dat partition.mbn partition_nand.xml** 三个文件是配合实现安全启动，不带签名的。

(1) 先烧录不带 sec.dat 文件



(2) 当模块正常启动，第二次再单独烧录 sec.dat