格式说明

证书格式参考 MshPRT_v1.1#5.5.1.1 Certificate format 章节内容

使用前准备

- macOS， Linux
    - 安装openssl
- windows
    - 安装gitbash（内含openssl）

使用方法

1. 生成root（根）证书：运行gen-root.bash 结果输出在 output-root 目录中。 一般只需要运行一次。
2. 生成intermediate（中间）证书：运行gen-intermediate.bash，该证书由根证书签名， 结果输出在 output-intermediate 目录中。 一般只需要运行一次。
3. 生成device（设备）证书：将设备的device UUID， CID和PID信息分别替换 gen-device.config 中的CN 对应字段，再运行gen-device.bash。该证书由中间证书签名， 结果输出在 output-device 目录中。 ~ 运行bash：在macOS,linux命令行或window的gitbash中输入./xxx.bash~

output-xx 内容说明

- xx-private.pem : 私钥文件， PEM格式
- xx-private.der : 私钥文件， DER格式
- xx-csr.csr : 请求文件
- xx.pem : 证书文件， PEM格式
- xx.der : 证书文件， DER格式
- readme.txt : readme文件

查看内容

- 查看私钥： openssl ec -noout -text -in xxx.der
- 查看请求文件： openssl req -text -noout -in xxx.csr
- 查看证书： openssl x509 -text -noout -in xxx.der

bin文件格式

- offset（0）： type(0x00,证书格式, 1个字节)
- offset（0x010）： device_cert(0x10,前4个字节是len)
- offset（0x700）： inter_midate_cert(0x700,前4个字节是len)
- offset（0xe00）： cert_pub_key（64字节）
- offset（0xe40）： cert_private_key（32个字节）
- offset（0xe60）： cert_uuid（16个字节）
- offset（0xe70）： cert_static_oob（32个字节， 暂未启用）
- offset（0xf00）： crc32.
- offset（0xf04）： valid flag.

~~旧版本~~

- ~~static oob: 在 gen_device.config#v3_req 中添加自定义字段，以支持staticoob字段: 2.25.234763379998062148653007332685657680359 = xxxx~~

version record

- 20231020: 修复public key写入位置错误问题
- 20231019: 修复crc生成校验数据错误问题
- 20231018: gen-device.bash 中添加自动生成4k bin文件操作
- 20231010: init version