【不完整证书链】存在证书链的CA证书如何导入设备（二）

证书 孔梦龙 2022-01-12 发表

组网及说明

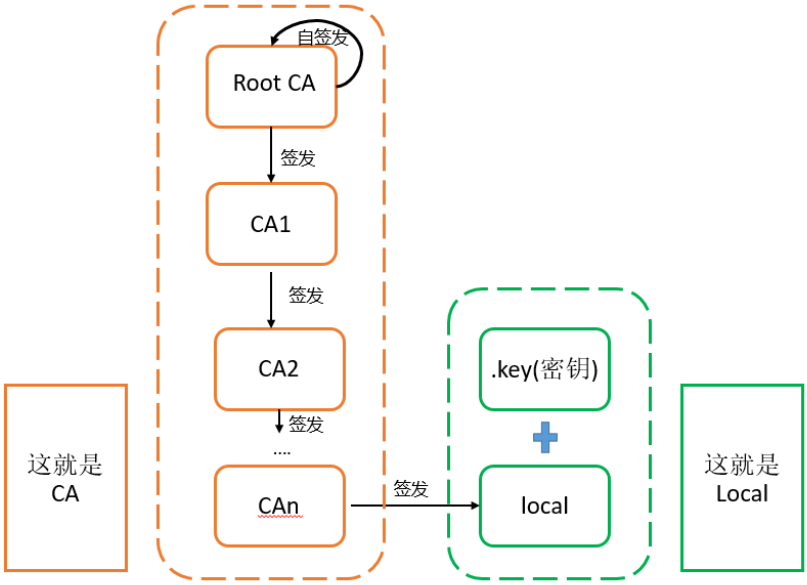
【不完整证书链】

完整的证书链必须有以下的情况：假设客户完整得提供了所有的证书，例如：根CA签发了CA1，CA1签发了CA2、CA2签发了CA3、CA3签发了local等等。客户把上面的CA、CA1、CA2、CA3、local和密钥key都提供了。（有些时候key已经合入了local）

什么是不完整的证书链呢？就是说上面客户仅提供了某一级CA，local和key，本应该完整的把CA1、CA2、CA3等之类的全部提供，但是就是没有完整发给我们；

注：这里假设您已经了解了CA证书、Local证书、私钥，PKI域等概念。
正常的情况下，一对证书会包含一个local证书和CA证书，但是现场客户提供了很多证书，存在证书链（就是上面CA1、CA2等）的情况，让导入到设备上，就需要先合成证书再导入。
所谓的证书链是指CA机构提供的CA证书并不是一个，而是由多级连续签发，存在根CA证书和被签发CA证书。这种情况下，为了获得完整有效的证书，需要将CA证书和local分别合成以后，再导入设备。

示意图：



配置步骤

1

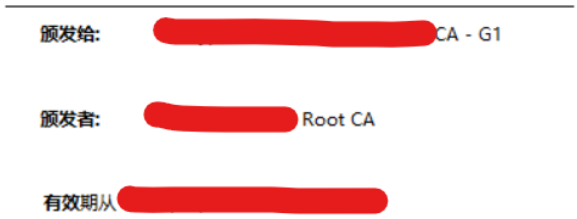
以下以某一局点的案例说明整个过程怎么操作；

- 客户提供的证书截图如下：

aaa.key	2022/1/12 8:54	KEY 文件	2 KB
ZS1.crt	2022/1/12 8:54	安全证书	2 KB
ZS2.crt	2022/1/12 8:55	安全证书	3 KB

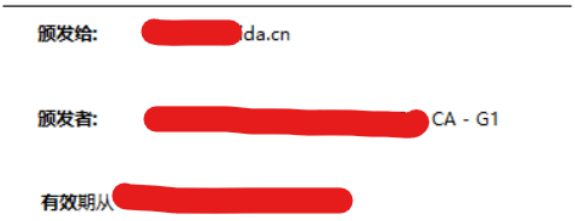
点开看证书的情况：

ZS1 的信息：



可以看到这个证书的颁发者是 Root CA，颁发给了 CA-G1

ZS2 的信息：



这个证书的颁发者是 CA-G1，颁发给了 da.cn 这个域名

总结：也是说 ROOT 签发了 CA-G1，CA-G1 签发了 da.cn，这样来看，ZS1 就是 CA（相当于示意图的 CA1），ZS2 就是 local，aaa.key 是 local 证书的密钥。但是对比示意图发现这个证书是不完整的，不完整之处在于 CA 不完整，需要根 Root CA。

- 我们的目的是什么？

（1） 获得完整的 CA = Root CA + CA-G1

（2） 获得完整的 Local = local + aaa.key

- 我们应该怎么做？

（1） 获得完整的 Local = local + aaa.key

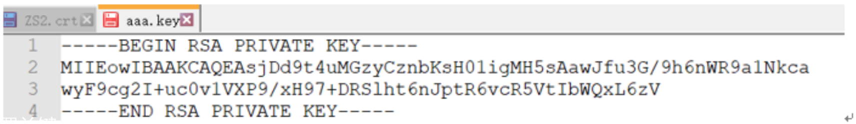
（有些时候，客户提供的证书已经将两者合成在一起了，合成一起的证书上会有钥匙的小图标，没有合成的就是一个小奖章的小图标）

第一步：找到 ZS2，使用 notepad++打开

ZS2.crt aaa.key

```
-----BEGIN CERTIFICATE-----
MIIF9zCCBN+gAwIBAgIQC3mkexIAC1Aaj1vEX/xuCTANBgkqhkiG9w0BAQsFADBu
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
29NbkKMeD77gvvs8V2cxTLPkI2gX9VUBcIMSyBNSTMr83phPQ+ITZ0zXiA==
-----END CERTIFICATE-----
```

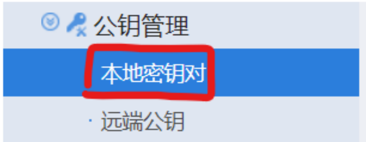
第二步：找到 aaa.key，使用 notepad++打开



第三步：将 aaa.key 的内容粘贴到 ZS2 最上面

1

如果提示密钥已存在之类的，那就是现场之前导入证书把 key 已经放进去了，需要在密钥处把这个删了，因为新的证书已经包含了；



（2） 获得完整的 CA = Root CA + CA-G1

附件下载怎样获得完整的 CA 呢？还是要深刻理解上面的示意图；上面的示意图中的各个模块缺一不可，比如我们给出的案例中 CA-G1 签发 da.cn，我们仅需要找到 Root CA 即可；

但是，万一客户给的是示意图中 CA2，也就是 CA2 向上接不住 Root CA，向下接不住 local，