



防火墙设备申请证书文件的导出方法

PKI

IPSec VPN

李瑞

2022-03-01 发表

组网及说明

不涉及

问题描述

申请ipsec证书时，有的CA机构要求我们防火墙设备提供pkcs10格式的crs文件用于证书申请，下边给出证书申请文件导出的方法

过程分析

离线申请，最后的pkcs10码拷贝到文本文件里，保存为.csr文件，即可到ca申请证书

注意如果不是国密证书，sm2改成rsa即可

public-key sm2 general name sm2z3-----配置指定证书申请使用的SM2密钥对的名称

public-key local create sm2 name sm2z3

1 cer格式证书离线申请及导入

1、配置PKI实体

```
[H3C-pki-entity-h3c1]dis this
```

```
#
```

```
pki entity h3c1
```

```
common-name z3
```

```
#
```

2、配置PKI域。

```
#
```

```
pki domain h3c1
```

```
certificate request entity h3c1-----配置用于申请证书的PKI实体
```

```
public-key sm2 general name sm2z3-----配置指定证书申请使用的SM2密钥对的名称
```

```
undo crl check enable-----关闭crl检查
```

```
#
```

```
return
```

```
[H3C-pki-domain-h3c1]
```

3、生成SM2密钥对

由于测试的是加密卡，因此生成密钥对时需指定加密卡，如果不指定由硬件加密卡生成密钥对，则测试的是软件SM2，验证不到加密卡。若使用密钥对申请了数字证书后便不能随便执行密钥对销毁操作，否则将导致使用此密钥对申请的证书与密钥对不匹配而不可用，即使销毁后再生成与之前名字相同的密钥对也是不可以的。

```
[H3C]public-key local create sm2 name sm2z3 on cndex2/2/1
```

```
Generating Keys...
```

```
....
```

```
Created the key pair successfully.
```

```
[H3C]dis public-key local sm2 public name sm2z3
```

```
=====
```

```
Key name: sm2z3
```

```
Key type: SM2
```

```
Storage device serial number: 0271016100250552
```

```
Time when key pair created: 09:52:38 2018/03/14
```

```
Key code:
```

```
04D60E8BECA1DF1F4551C0C039A5C206A3D598BCEE58761DF427DF1847BCE9B6FE717940D  
B
```

```
9BC310563FA9931DCEA225BCD09224FD8CF173DAF26E0CC4F79DFCCB
```

4、生成申请离线证书的pkcs10码发送给CA服务器。

```
[H3C]pki request-certificate domain h3c1 pkcs10
```

```
.
```

```
*** Request for general certificate ***
```

```
-----BEGIN CERTIFICATE REQUEST-----
```

```
MIHoMIGNAgEAMA0xCzAJBgNVBAMTAnozMFkwEwYHKoZIzj0CAQYIKoEcz1UBgi0D  
QgAE1g6L7KHfH0VRwMA5pclGo9WYvO5Ydh30J98YR7zptv5xeUDbm8MQVj+pkx3O  
oiW80Jlk/Yzxc9rybgzE9538y6AeMBWGCsQGSIb3DQEJDjEPMA0wCwYDVz0PBAQD  
AgP4MAAwGCCqBHM9VAYN1BQADSAAwRQIgf5gklpc9L22s+hmjsUAnsfpwphusSiZNLZ  
33hrMNdvaqkCIQDLK8qVX62dQDsWMfNyv6Jg/q5FE9qiAFUboPj1t6oX8w==
```

```
-----END CERTIFICATE REQUEST-----
```

解决方法

按照如上方法导出申请证书用的文件即可

