

1、使用openssl生成证书时配置文件注意事项（在原有的配置文件中加上）

```
[req]
req_extensions = v3_req
[v3_req]
subjectAltName = @alt_names
[alt_names]
DNS.1 = 169.254.0.17
IP.1 = 169.254.0.17
```

2、上传证书功能:

根据 openssl 生成CA私钥

```
openssl genrsa -out ca.key 2048
```

使用CA私钥生成CA根证书 -----> 给BIOS(通过BIOS setup 中的接口上传)

```
openssl req -x509 -sha256 -new -nodes -config openssl.cnf -key ca.key -days 3650
-out ca.crt -subj
/C=CN/ST=Georgia/L=Norcross/O=ccbx/OU=ServiceProcessors/CN=cbx.com/emailAddress=
1694313328@qq.com
```

根据 openssl 生成服务器私钥 -----> 通过web上传证书功能上传

```
openssl genrsa -out server.key 1024
```

生成服务器的证书请求文件（CSR），并在里面配置域名和IP（BIOS访问的 IP.1 = 169.254.0.17）

```
openssl req -new -key server.key -out server.csr -config openssl.cnf -subj
/C=CN/ST=Georgia/L=Norcross/O=scbx/OU=ServiceProcessors/CN=cbx.com/emailAddress=
1694313328@qq.com
```

根据CA私钥和CSR文件生成服务器证书 -----> 通过web上传证书功能上传

```
openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out
server.crt -days 3650 -extfile openssl.cnf -extensions v3_req
```

3、生成证书功能:

将BMC/conf目录下的actualcert.pem ----> 给BIOS(通过BIOS setup 中的接口上传)

actualcert.pem文件可以通过web一键收集下载到（下载解压后的/conf/actualcert.pem）



