证书标准

X.509 - 这是一种证书标准,主要定义了证书中应该包含哪些内容.其详情可以参考RFC5280,SSL使用的就是这种证书标准. 证书包含有RSA公匙信息

编码格式

同样的X.509证书,可能有不同的编码格式,目前有以下两种编码格式.

PEM - Privacy Enhanced Mail,打开看文本格式,以"-----BEGIN..."开头, "-----END..."结尾,内容是BASE64编码.  
 查看PEM格式证书的信息:openssl x509 -in certificate.pem -text -noout

DER - Distinguished Encoding Rules,打开看是二进制格式,不可读.  
查看DER格式证书的信息:openssl x509 -in certificate.der -inform der -text -noout

相关的文件扩展名

这是比较误导人的地方,虽然我们已经知道有PEM和DER这两种编码格式,但文件扩展名并不一定就叫"PEM"或者"DER",常见的扩展名除了PEM和DER还有以下这些,它们除了编码格式可能不同之外,内容也有差别,但大多数都能相互转换编码格式.

CRT - CRT应该是certificate的三个字母,其实还是证书的意思,常见于\*NIX系统,有可能是PEM编码,也有可能是DER编码,大多数应该是PEM编码,相信你已经知道怎么辨别.

CER - 还是certificate,还是证书,常见于Windows系统,同样的,可能是PEM编码,也可能是DER编码,大多数应该是DER编码.

KEY - 通常用来存放一个公钥或者私钥,并非X.509证书,编码同样的,可能是PEM,也可能是DER.  
 查看KEY的办法:openssl rsa -in mykey.key -text -noout  
 如果是DER格式的话,同理应该这样了:openssl rsa -in mykey.key -text -noout -inform der

CSR - Certificate Signing Request,即证书签名请求,这个并不是证书,而是向权威证书颁发机构获得签名证书的申请,其核心内容是一个公钥(当然还附带了一些别的信息)

查看的办法:openssl req -noout -text -in my.csr (如果是DER格式的话照旧加上-inform der,这里不写了)

PFX/P12 - predecessor of PKCS#12,对\*nix服务器来说,一般CRT和KEY是分开存放在不同文件中的,但Windows的IIS则将它们存在一个PFX文件中(因此这个文件包含了证书及私钥),PFX通常会有一个"提取密码",你想把里面的东西读取出来的话,它就要求你提供提取密码,PFX使用的是DER编码,如何把PFX转换为PEM编码？  
 openssl pkcs12 -in for-iis.pfx -out for-iis.pem -nodes  
 这个时候会提示你输入提取代码. for-iis.pem就是可读的文本.

证书编码的转换

PEM转为DER openssl x509 -in cert.crt -outform der -out cert.der

DER转为PEM openssl x509 -in cert.crt -inform der -outform pem -out cert.pem