Atitti.数字证书体系attilax总结

[一、数字证书常见标准 1](#_Toc5357)

[数字证书文件格式（cer和pfx）的区别： 1](#_Toc3516)

[二、数字证书存储内容 2](#_Toc20212)

[X.509是一种非常通用的证书格式。 2](#_Toc14285)

[详细特征 2](#_Toc10609)

[X.509证书格式 3](#_Toc31468)

## 一、数字证书常见标准

数字证书体现为一个或一系列相关经过加密的数据文件。常见格式有：

* 符合PKI ITU-T X509标准，传统标准（.DER .PEM .CER .CRT）
* 符合PKCS#7 加密消息语法标准(.P7B .P7C .SPC .P7R)
* 符合PKCS#10 证书请求标准(.p10)
* 符合PKCS#12 个人信息交换标准（.pfx \*.p12）

当然，这只是常用的几种标准，其中，X509证书还分两种编码形式：

* X.509 DER(Distinguished Encoding Rules)编码，后缀为： .DER .CER .CRT
* X.509 BASE64编码，后缀为： .PEM .CER .CRT

X509是数字证书的基本规范，而P7和P12则是两个实现规范，P7用于数字信封，P12则是带有私钥的证书实现规范

## 数字证书文件格式（cer和pfx）的区别：

由定义可以看出，只有pfx格式的数字证书是包含有私钥的，cer格式的数字证书里面只有公钥没有私钥。

Windows下常见两种证书，后缀为.cer的通常存放公钥，后缀为.pfx的通常存放私钥。有时候想看一下其中内容到底是什么，又不想写程序，这个时候OpenSSL的命令行工具就很有用了。

.cer格式比较好处理，它就是一个x509证书，openssl直接可以处理，只需要执行

## 二、数字证书存储内容

采用的标准不同，生成的数字证书，包含内容也可能不同。

下面就证书包含/可能包含的内容做个汇总，一般证书特性有：

* 存储格式：二进制还是ASCII
* 是否包含公钥、私钥
* 包含一个还是多个证书
* 是否支持密码保护（针对当前证书）

其中：

* \*.der/\*.cer/\*.crt 以**二进制形式存放证书，只有公钥，不包含私钥。**
* \*.csr 证书请求
* \*.pem 以Base64编码形式存放证书，以"-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----"封装，只有公钥。
* \*.pfx/\*.p12也是以二进制形式存放证书，包含公钥、私钥，包含保护密码。pfx和p12存储格式完全相同只是扩展名不同。
* \*.p10 证书请求
* \*.p7r CA对证书请求回复，一般做数字信封
* \*.p7b/\*.p7c 证书链，可包含一个或多个证书。

**理解关键点：**

* 凡是包含私钥的，一律必须添加密码保护（加密私钥），因为按照习惯，公钥是可以公开的，私钥必须保护，所以明码证书以及未加保护的证书都不可能包含私钥，只有公钥，不用加密。
* 上文描述中，\*.der均表示证书且有签名，实际使用中，还有DER编码的私钥不用签名，实际上只是个“中间件”。

## X.509是一种非常通用的证书格式。

所有的证书都符合ITU-T X.509国际标准，因此(理论上)为一种应用创建的证书可以用于任何其他符合X.509标准的应用。

## 详细特征

[编辑](http://baike.baidu.com/javascript:;)

所有的X.509证书包含以下数据：　1、X.509版本号：指出该证书使用了哪种版本的X.509标准，版本号会影响证书中的一些特定信息。目前的版本是3。

2、证书持有人的[公钥](http://baike.baidu.com/view/355291.htm" \t "http://baike.baidu.com/_blank)：包括证书持有人的公钥、算法(指明密钥属于哪种密码系统)的标识符和其他相关的密钥参数。

3、证书的序列号：由CA给予每一个证书分配的唯一的数字型编号，当证书被取消时，实际上是将此证书序列号放入由CA签发的CRL（Certificate Revocation List证书作废表，或证书黑名单表）中。这也是序列号唯一的原因。

4、主题信息：证书持有人唯一的标识符(或称DN-distinguished name)这个名字在 Internet上应该是唯一的。DN由许多部分组成，看起来象这样：

CN=Bob Allen, OU=Total Network Security Division

O=Network Associates, Inc.

C=US

这些信息指出该科目的通用名、组织单位、组织和国家或者证书持有人的姓名、服务处所等信息。

5、证书的有效期：证书起始日期和时间以及终止日期和时间；指明证书在这两个时间内有效。

6、认证机构：证书发布者，是签发该证书的实体唯一的CA的X.509名字。使用该证书意味着信任签发证书的实体。(注意：在某些情况下，比如根或顶级CA证书，发布者自己签发证书)

7、发布者的数字签名：这是使用发布者[私钥](http://baike.baidu.com/view/493846.htm" \t "http://baike.baidu.com/_blank)生成的签名，以确保这个证书在发放之后没有被撰改过。

8、签名算法标识符：用来指定CA签署证书时所使用的签名算法。算法标识符用来指定CA签发证书时所使用的[公开密钥](http://baike.baidu.com/view/1145160.htm" \t "http://baike.baidu.com/_blank)算法和HASH算法。

## X.509证书格式

为了利用[公共密钥](http://baike.baidu.com/view/11755775.htm" \t "http://baike.baidu.com/_blank)这种密码系统，必须将公共密钥分发出去。最通用的一种签名证书格式被称为X.509格式

Ref参考资料

Byekle

X509证书 - wyxhd2008的专栏 - 博客频道 - CSDN.NET.html