[**PKCS 发布的15 个标准**](http://falchion.iteye.com/blog/1472453)

PKCS 全称是 Public-Key Cryptography Standards ，是由 RSA 实验室与其它安全系统开发商为促进公钥密码的发展而制订的一系列标准。

可以到官网上看看 [What is PKCS](http://www.rsa.com/rsalabs/node.asp?id=2308)

PKCS 目前共发布过 15 个标准：  
（1）PKCS#1：RSA加密标准。PKCS#1定义了RSA公钥函数的基本格式标准，特别是数字签名。它定义了数字签名如何计算，包括待签名数据和签名本身的格式；它也定义了PSA公/私钥的语法。  
  
（2）PKCS#2：涉及了RSA的消息摘要加密，这已被并入PKCS#1中。  
  
（3）PKCS#3：Diffie-Hellman密钥协议标准。PKCS#3描述了一种实现Diffie- Hellman密钥协议的方法。  
  
（4）PKCS#4：最初是规定RSA密钥语法的，现已经被包含进PKCS#1中。  
  
（5）PKCS#5：基于口令的加密标准。PKCS#5描述了使用由口令生成的密钥来加密8位位组串并产生一个加密的8位位组串的方法。PKCS#5可以用于加密私钥，以便于密钥的安全传输（这在PKCS#8中描述）。  
  
（6）PKCS#6：扩展证书语法标准。PKCS#6定义了提供附加实体信息的X.509证书属性扩展的语法（当PKCS#6第一次发布时，X.509还不支持扩展。这些扩展因此被包括在X.509中）。  
  
（7）PKCS#7：密码消息语法标准。PKCS#7为使用密码算法的数据规定了通用语法，比如数字签名和数字信封。PKCS#7提供了许多格式选项，包括未加密或签名的格式化消息、已封装（加密）消息、已签名消息和既经过签名又经过加密的消息。  
  
（8）PKCS#8：私钥信息语法标准。PKCS#8定义了私钥信息语法和加密私钥语法，其中私钥加密使用了PKCS#5标准。  
  
（9）PKCS#9：可选属性类型。PKCS#9定义了PKCS#6扩展证书、PKCS#7数字签名消息、PKCS#8私钥信息和PKCS#10证书签名请求中要用到的可选属性类型。已定义的证书属性包括E-mail地址、无格式姓名、内容类型、消息摘要、签名时间、签名副本（counter signature）、质询口令字和扩展证书属性。  
  
（10）PKCS#10：证书请求语法标准。PKCS#10定义了证书请求的语法。证书请求包含了一个唯一识别名、公钥和可选的一组属性，它们一起被请求证书的实体签名（证书管理协议中的PKIX证书请求消息就是一个PKCS#10）。  
  
（11）PKCS#11：密码令牌接口标准。PKCS#11或“Cryptoki”为拥有密码信息（如加密密钥和证书）和执行密码学函数的单用户设备定义了一个应用程序接口（API）。智能卡就是实现Cryptoki的典型设备。注意：Cryptoki定义了密码函数接口，但并未指明设备具体如何实现这些函数。而且Cryptoki只说明了密码接口，并未定义对设备来说可能有用的其他接口，如访问设备的文件系统接口。  
  
（12）PKCS#12：个人信息交换语法标准。PKCS#12定义了个人身份信息（包括私钥、证书、各种秘密和扩展字段）的格式。PKCS#12有助于传输证书及对应的私钥，于是用户可以在不同设备间移动他们的个人身份信息。  
  
（13）PDCS#13：椭圆曲线密码标准。PKCS#13标准当前正在完善之中。它包括椭圆曲线参数的生成和验证、密钥生成和验证、数字签名和公钥加密，还有密钥协定，以及参数、密钥和方案标识的ASN.1语法。  
  
（14）PKCS#14：伪随机数产生标准。PKCS#14标准当前正在完善之中。为什么随机数生成也需要建立自己的标准呢？PKI中用到的许多基本的密码学函数，如密钥生成和Diffie-Hellman共享密钥协商，都需要使用随机数。然而，如果“随机数”不是随机的，而是取自一个可预测的取值集合，那么密码学函数就不再是绝对安全了，因为它的取值被限于一个缩小了的值域中。因此，安全伪随机数的生成对于PKI的安全极为关键。  
  
（15）PKCS#15：密码令牌信息语法标准。PKCS#15通过定义令牌上存储的密码对象的通用格式来增进密码令牌的互操作性。在实现PKCS#15的设备上存储的数据对于使用该设备的所有应用程序来说都是一样的，尽管实际上在内部实现时可能所用的格式不同。PKCS#15的实现扮演了翻译家的角色，它在卡的内部格式与应用程序支持的数据格式间进行转换。

**X509**

X.509是常见通用的证书格式。所有的证书都符合为Public Key Infrastructure (PKI) 制定的 ITU-T X509 国际标准。X.509是国际电信联盟-电信（ITU-T）部分标准和国际标准化组织（ISO）的证书格式标准。作为ITU-ISO目录服务系列标准的一部分，X.509是定义了公钥证书结构的基本标准。1988年首次发布，1993年和1996年两次修订。当前使用的版本是X.509 V3，它加入了扩展字段支持，这极大地增进了证书的灵活性。X.509 V3证书包括一组按预定义顺序排列的强制字段，还有可选扩展字段，即使在强制字段中，X.509证书也允许很大的灵活性，因为它为大多数字段提供了多种编码方案.

PKCS#7 常用的后缀是： .P7B .P7C .SPC

PKCS#12 常用的后缀有： .P12 .PFX

X.509 DER 编码(ASCII)的后缀是： .DER .CER .CRT

X.509 PAM 编码(Base64)的后缀是： .PEM .CER .CRT

.cer/.crt是用于存放证书，它是2进制形式存放的，不含私钥。

.pem跟crt/cer的区别是它以Ascii来表示。

pfx/p12用于存放个人证书/私钥，他通常包含保护密码，2进制方式

p10是证书请求

p7r是CA对证书请求的回复，只用于导入

p7b以树状展示证书链(certificate chain)，同时也支持单个证书，不含私钥。

一 用openssl创建CA证书的RSA密钥(PEM格式)：  
openssl genrsa -des3 -out ca.key 1024

二用openssl创建CA证书(PEM格式,假如有效期为一年)：  
openssl req -new -x509 -days 365 -key ca.key -out ca.crt -config openssl.cnf  
openssl是可以生成DER格式的CA证书的，最好用IE将PEM格式的CA证书转换成DER格式的CA证书。

三 x509到pfx  
pkcs12 -export –in keys/client1.crt -inkey keys/client1.key -out keys/client1.pfx

四 PEM格式的ca.key转换为Microsoft可以识别的pvk格式。  
  pvk -in ca.key -out ca.pvk -nocrypt -topvk

五 PKCS#12 到 PEM 的转换  
openssl pkcs12 -nocerts -nodes -in cert.p12 -out private.pem  
验证 openssl pkcs12 -clcerts -nokeys -in cert.p12 -out cert.pem

六 从 PFX 格式文件中提取私钥格式文件 (.key)  
openssl pkcs12 -in mycert.pfx -nocerts -nodes -out mycert.key

七 转换 pem 到到 spc  
openssl crl2pkcs7 -nocrl -certfile venus.pem  -outform DER -out venus.spc  
用 -outform -inform 指定 DER 还是 PAM 格式。例如：  
openssl x509 -in Cert.pem -inform PEM -out cert.der -outform DER

八 PEM 到 PKCS#12 的转换，  
openssl pkcs12 -export -in Cert.pem -out Cert.p12 -inkey key.pem

**密钥库文件格式【Keystore】**

 格式     :  JKS  
 扩展名  : .jks/.ks  
 描述     : 【Java Keystore】密钥库的Java实现版本，provider为SUN  
 特点     :  密钥库和私钥用不同的密码进行保护  
   
 格式     :  JCEKS  
 扩展名  :  .jce  
 描述     : 【JCE Keystore】密钥库的JCE实现版本，provider为SUN JCE  
 特点     :  相对于JKS安全级别更高，保护Keystore私钥时采用TripleDES  
   
 格式     :  PKCS12  
 扩展名  :  .p12/.pfx  
 描述     : 【PKCS #12】个人信息交换语法标准  
 特点     :  1、包含私钥、公钥及其证书  
               2、密钥库和私钥用相同密码进行保护  
   
 格式     :  BKS  
 扩展名  : .bks  
 描述     :  Bouncycastle Keystore】密钥库的BC实现版本，provider为BC  
 特点     :  基于JCE实现  
   
 格式     : UBER  
 扩展名  : .ubr  
 描述     : 【Bouncycastle UBER Keystore】密钥库的BC更安全实现版本，provider为BC

**证书文件格式【Certificate】**

格式          :  DER   
扩展名       :  .cer/.crt/.rsa

描述          : 【ASN .1 DER】用于存放证书   
特点          :  不含私钥、二进制

格式          :  PKCS7   
扩展名       : .p7b/.p7r   
描述          : 【PKCS #7】加密信息语法标准

特点          : 1、p7b以树状展示证书链，不含私钥  
                  2、p7r为CA对证书请求签名的回复，只能用于导入

格式          :  CMS   
扩展名       :  .p7c/.p7m/.p7s   
描述          : 【Cryptographic Message Syntax】   
特点          : 1、p7c只保存证书  
                  2、p7m：signature with enveloped data  
                  3、p7s：时间戳签名文件  
   
格式          :  PEM  
扩展名       : .pem   
描述          : 【Printable Encoded Message】   
特点          : 1、该编码格式在RFC1421中定义，其实PEM是【Privacy-Enhanced Mail】的简写，但他也同样广泛运用于密钥管理  
                  2、ASCII文件  
                  3、一般基于base 64编码

格式         :  PKCS10   
扩展名      : .p10/.csr   
描述         : 【PKCS #10】公钥加密标准【Certificate Signing Request】  
特点         :  1、证书签名请求文件  
                  2、ASCII文件  
                  3、CA签名后以p7r文件回复

格式         :  SPC   
扩展名      : .pvk/.spc   
描述         : 【Software Publishing Certificate】   
特点         :  微软公司特有的双证书文件格式，经常用于代码签名，其中  
                  1、pvk用于保存私钥  
                  2、spc用于保存公钥