

公钥证书编码解读

一、文件编码

PEM (Privacy Enhancement Message), 定义见 [RFC1421](#)
是一种基于 base64 的编码格式，常见于 linux/unix 下的证书编码

结构组成 == {header} body {tail}
示例

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDMYfnvWtC8Id5bPKae5yXSxQTt
+Zpul6AnnZWfI2TtIarvjHBFUtXR096y7hoL4VWOPKGCsRqMFDkrbeUjRrx8iL9l
4/srnyf6sh9c8Zk04xEOPk1ypvBz+Ks4uZObtjnnitf0NBGdjMKxveTq+VE7BWUI
yQjtQ8mbDOsiLLvh7wIDAQAB
-----END PUBLIC KEY-----
```

DER (Distinguished Encoding Rules), 定义见[维基百科-ASN.1.DER](#)
是来自ASN.1 体系的一种二进制编码格式，常用于 windows/mac 的证书编码
编码方式 == DER uses a pattern of type-length-value triplets

二、公钥标准

PKCS (Public Key Cryptography Standards), 定义见[维基百科-PKCS](#)
是一套公钥密码学标准，其定义范围涵盖了证书签名、加密算法、填充模式及校验流程等。
常见**PKCS**标准

公告



美码师，老码农一枚，
喜欢聊聊代码，唠唠职场
故事，爱技术也爱生活
欢迎关注我的公众号

Visitors

See more ▶

 127,281	 1,032	 120
 4,067	 534	 105
 2,977	 198	
 1,129	 160	

FLAG counter

昵称：美码师
园龄：8年5个月
粉丝：90
关注：7
+加关注

<	2019年6月						>
日	一	二	三	四	五	六	
26	27	28	29	30	31	1	
2	3	4	5	6	7	8	
9	10	11	12	13	14	15	
16	17	18	19	20	21	22	
23	24	25	26	27	28	29	

版本	里程碑
PKCS #1	RFC8017, 定义了公钥私钥的编码格式(ASN.1编码), 包括基础算法及编码/填充模式、签名校验, openssl 的默认标准格式
PKCS #3	DiffieHellman Key Agreement, 定义了DH 密钥交换标准
PKCS #5	RFC8018, 基于密码的加密标准, 定义了PBKDF2算法
PKCS #7	RFC2315, 定义密钥信息语法标准, PKI体系下的信息签名及加密标准, 是S/MIME的一部分
PKCS #8	RFC5958, 定义私钥信息语法标准, 用于描述证书密钥对的通用格式(不限RSA)
PKCS #11	定义了密钥 Token接口, 常用于单点登录/公钥算法/磁盘加密系统.(硬件加密)
PKCS #12	RFC7292, 个人信息交换语法标准, 定义了私钥和公钥证书的存储方式(支持密码), 常用 PFX简称, Java Key Store的编码格式

三、RSA 密钥

RSA 公钥编码

PublicKey-PKCS#1-PEM

```
-----BEGIN RSA PUBLIC KEY-----  
BASE64 ENCODED DATA  
-----END RSA PUBLIC KEY-----
```

PublicKey-PKCS#1-DER

```
RSAPublicKey ::= SEQUENCE {  
    modulus          INTEGER,  -- n  
    publicExponent   INTEGER   -- e  
}
```

PublicKey-PKCS#8-PEM

```
-----BEGIN PUBLIC KEY-----  
BASE64 ENCODED DATA  
-----END PUBLIC KEY-----
```

PublicKey-PKCS#8-DER

```
PublicKeyInfo ::= SEQUENCE {  
    algorithm      AlgorithmIdentifier,  
    PublicKey      BIT STRING  
}  
  
AlgorithmIdentifier ::= SEQUENCE {  
    algorithm      OBJECT IDENTIFIER,  
    parameters     ANY DEFINED BY algorithm OPTIONAL  
}
```

对于RSA公钥来说，OID就是(1.2.840.113549.1.1.1)

RSA 私钥编码

PrivateKey-PKCS#1-PEM

```
-----BEGIN RSA PRIVATE KEY-----  
BASE64 ENCODED DATA  
-----END RSA PRIVATE KEY-----
```

PrivateKey-PKCS#1-DER

```

RSAPrivateKey ::= SEQUENCE {
    version          Version,
    modulus           INTEGER,  -- n
    publicExponent    INTEGER,  -- e
    privateExponent   INTEGER,  -- d
    prime1            INTEGER,  -- p
    prime2            INTEGER,  -- q
    exponent1         INTEGER,  -- d mod (p-1)
    exponent2         INTEGER,  -- d mod (q-1)
    coefficient        INTEGER,  -- (inverse of q) mod p
    otherPrimeInfos    OtherPrimeInfos OPTIONAL
}

```

PrivateKey-PKCS#8-PEM

```

-----BEGIN PRIVATE KEY-----
BASE64 ENCODED DATA
-----END PRIVATE KEY-----

```

PrivateKey-PKCS#8-DER

```

PrivateKeyInfo ::= SEQUENCE {
    version          Version,
    algorithm         AlgorithmIdentifier,
    PrivateKey       OCTET STRING
}

AlgorithmIdentifier ::= SEQUENCE {
    algorithm        OBJECT IDENTIFIER,
    parameters       ANY DEFINED BY algorithm OPTIONAL
}

```

私钥文件可采用加密方式存储，加密后的格式：

EncryptedPrivateKey-PKCS#8-PEM

```
-----BEGIN ENCRYPTED PRIVATE KEY-----  
BASE64 ENCODED DATA  
-----END ENCRYPTED PRIVATE KEY-----
```

Encrypted-PrivateKey-PKCS#8-DER

```
EncryptedPrivateKeyInfo ::= SEQUENCE {  
    encryptionAlgorithm  EncryptionAlgorithmIdentifier,  
    encryptedData         EncryptedData  
}  
  
EncryptionAlgorithmIdentifier ::= AlgorithmIdentifier  
  
EncryptedData ::= OCTET STRING
```

四、证书

X.509 证书, [维基百科-X.509](#), 是目前流行的公钥证书标准。

一个 X.509 证书包含了一个公钥和对应的实体名(hostname/organization/individual); 证书通常由证书认证机构签名或自签名; 当证书持有者被另外一方信任时(通过公钥签名验证), 两者便可以基于公钥算法建立安全传输通道。

证书结构

```
Certificate  
Version Number  
Serial Number  
Signature Algorithm ID  
Issuer Name  
Validity period  
Not Before  
Not After  
Subject name  
Subject Public Key Info  
Public Key Algorithm  
Subject Public Key
```

```
Issuer Unique Identifier (optional)
Subject Unique Identifier (optional)
Extensions (optional)
...
Certificate Signature Algorithm
Certificate Signature
```

主要字段

字段	描述
版本号	指出该证书使用了哪种版本的X.509标准（版本1、版本2或是版本3），版本号会影响证书中的一些特定信息
序列号	标识证书的唯一整数，由证书颁发者分配的本证书的唯一标识符
签名算法标识符	用于签证书的算法标识，由对象标识符加上相关的参数组成，用于说明本证书所用的数字签名算法。例如，SHA-1-RSA
颁发者名称	证书颁发者的可识别名（DN），是签发该证书的实体唯一的CA的X.500名字
有效期限	证书起始日期和时间以及终止日期和时间
主体名	证书持有人的唯一标识符(或称DN-distinguished name)
公钥信息	包括证书持有人的公钥、算法
颁发者唯一标识符	标识符—证书颁发者的唯一标识符，仅在版本2和版本3中有要求，属于可选项
主体唯一标识符	标识符—证书颁发者的唯一标识符，仅在版本2和版本3中有要求，属于可选项

字段	描述
颁发者的数字签名	这是使用颁发者私钥生成的签名，以确保这个证书在发放之后没有被篡改过
扩展信息	..

扩展字段

字段	描述
发行者密钥标识符	证书所含密钥的唯一标识符，用来区分同一证书拥有者的多对密钥
密钥使用	一个比特串，指明（限定）证书的公钥可以完成的功能或服务，如：证书签名、数据加密等。如果某一证书将 KeyUsage 扩展标记为“极重要”，而且设置为“keyCertSign”，则在 SSL 通信期间该证书出现时将被拒绝，因为该证书扩展表示相关私钥应只用于签写证书，而不应该用于 SSL

字段	描述
C R L 分 布 点	指明CRL的分布地点
私 钥 的 使 用 期	指明证书中与公钥相联系的私钥的使用期限，它也有Not Before和Not After组成。若此项不存在时，公私钥的使用期是一样的
证 书 策 略	由对象标识符和限定符组成，这些对象标识符说明证书的颁发和使用策略有关
策 略 映 射	表明两个CA域之间的一个或多个策略对象标识符的等价关系，仅在CA证书里存在

字段	描述
主体别名	指出证书拥有者的别名，如电子邮件地址、IP地址等，别名是和DN绑定在一起的
颁发者别名	指出证书颁发者的别名，如电子邮件地址、IP地址等，但颁发者的DN必须出现在证书的颁发者字段
主体目录属性	指出证书所有者的一系列属性。可以使用这一项来传递访问控制信息

样例-维基百科证书

```

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      10:e6:fc:62:b7:41:8a:d5:00:5e:45:b6
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation CA
- SHA256 - G2
    Validity

```

```
Not Before: Nov 21 08:00:00 2016 GMT
Not After : Nov 22 07:59:59 2017 GMT
Subject: C=US, ST=California, L=San Francisco, O=Wikimedia Foundation,
Inc., CN=*.wikipedia.org
Subject Public Key Info:
Public Key Algorithm: id-ecPublicKey
Public-Key: (256 bit)
pub:
    04:c9:22:69:31:8a:d6:6c:ea:da:c3:7f:2c:ac:a5:
    af:c0:02:ea:81:cb:65:b9:fd:0c:6d:46:5b:c9:1e:
    ed:b2:ac:2a:1b:4a:ec:80:7b:e7:1a:51:e0:df:f7:
    c7:4a:20:7b:91:4b:20:07:21:ce:cf:68:65:8c:c6:
    9d:3b:ef:d5:c1
ASN1 OID: prime256v1
X509v3 extensions:
X509v3 Key Usage: critical
    Digital Signature, Key Agreement
Authority Information Access:
    CA Issuers -
URI:http://secure.globalsign.com/cacert/gsorganizationvalsha2g2r1.crt
    OCSP - URI:http://ocsp2.globalsign.com/gsorganizationvalsha2g2

X509v3 Certificate Policies:
    Policy: 1.3.6.1.4.1.4146.1.20
    CPS: https://www.globalsign.com/repository/
    Policy: 2.23.140.1.2.2

X509v3 Basic Constraints:
    CA:FALSE
X509v3 CRL Distribution Points:

    Full Name:
        URI:http://crl.globalsign.com/gs/gsorganizationvalsha2g2.crl

X509v3 Subject Alternative Name:
    DNS:*.wikipedia.org, DNS:*.m.mediawiki.org, DNS:*.m.wikibooks.org,
    DNS:*.m.wikidata.org, DNS:*.m.wikimedia.org, DNS:*.m.wikimediafoundation.org,
```

```
DNS:*.m.wikinews.org, DNS:*.m.wikipedia.org, DNS:*.m.wikiquote.org,
DNS:*.m.wikisource.org, DNS:*.m.wikiversity.org, DNS:*.m.wikivoyage.org,
DNS:*.m.wiktionary.org, DNS:*.mediawiki.org, DNS:*.planet.wikimedia.org,
DNS:*.wikibooks.org, DNS:*.wikidata.org, DNS:*.wikimedia.org,
DNS:*.wikimediafoundation.org, DNS:*.wikinews.org, DNS:*.wikiquote.org,
DNS:*.wikisource.org, DNS:*.wikiversity.org, DNS:*.wikivoyage.org,
DNS:*.wiktionary.org, DNS:*.wmfusercontent.org, DNS:*.zero.wikipedia.org,
DNS:mediawiki.org, DNS:w.wiki, DNS:wikibooks.org, DNS:wikidata.org,
DNS:wikimedia.org, DNS:wikimediafoundation.org, DNS:wikinews.org,
DNS:wikiquote.org, DNS:wikisource.org, DNS:wikiversity.org, DNS:wikivoyage.org,
DNS:wiktionary.org, DNS:wmfusercontent.org, DNS:wikipedia.org
X509v3 Extended Key Usage:
    TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Subject Key Identifier:
    28:2A:26:2A:57:8B:3B:CE:B4:D6:AB:54:EF:D7:38:21:2C:49:5C:36
X509v3 Authority Key Identifier:
    keyid:96:DE:61:F1:BD:1C:16:29:53:1C:C0:CC:7D:3B:83:00:40:E6:1A:7C

Signature Algorithm: sha256WithRSAEncryption
8b:c3:ed:d1:9d:39:6f:af:40:72:bd:1e:18:5e:30:54:23:35:
66:5e:62:d5:01:e2:63:47:70:cb:6d:1b:17:b0:f5:4d:11:e4:
ad:94:51:c5:5e:72:03:b0:d5:ab:18:eb:b5:3a:08:a8:73:95:
f3:7f:41:1a:28:7b:45:7c:83:2e:d3:14:95:d8:d5:d1:5f:99:
4b:0c:f4:c3:9b:0b:4f:e9:49:f4:2c:b5:ae:c3:1d:7d:2a:80:
f6:70:29:4c:0c:e6:e0:cb:88:8a:8a:02:ee:a5:d1:73:c2:93:
58:24:ff:43:1b:e3:fd:7b:aa:f0:15:0c:60:52:8f:21:7d:87:
3a:14:fa:81:41:00:60:4f:96:9a:62:94:58:de:cb:15:5c:3c:
f4:c1:4d:33:e3:ff:39:fe:28:fb:b0:41:3e:d2:8a:11:d1:06:
01:28:74:7d:71:d4:2a:ef:1f:e3:25:4b:2d:f0:66:ef:26:fb:
4c:f0:81:85:bb:1a:99:06:c9:37:87:de:8d:49:f7:00:91:a9:
42:31:4a:b9:40:a0:7d:4f:4f:a6:ea:d4:58:07:3c:01:e0:1a:
53:54:66:e1:a3:7e:30:cd:3b:f8:69:59:a3:48:92:48:e1:9e:
63:ab:08:70:91:f2:48:d2:83:4b:98:06:fa:fd:bc:99:02:da:
9c:98:b1:a3
```

证书格式

- PKI ITU-T X509标准, 传统标准 (.der .pem .cer .crt) , 仅包含公钥
- PKCS#7 加密消息语法标准(.p7b .p7c .spc .p7r), p7b/p7c/spc 包含了证书链, p7r是证书请求回复(非证书)
- PKCS#10 证书请求标准(.p10), .p10是证书请求文件, 与.csr文件类似
- PKCS#12 个人信息交换标准 (.pfx *.p12) , 包含公钥和私钥, 需密码保护

编码形式

- X.509 DER(Distinguished Encoding Rules)编码, 后缀为: .der .cer .crt
- X.509 BASE64编码(PEM格式), 后缀为: .pem .cer .crt

X.509CRT-PEM

```
-----BEGIN CERTIFICATE-----  
BASE64 ENCODED DATA  
-----END CERTIFICATE-----
```

关键特性

- 编码形式: 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)

参考文档

[mbed文档-公钥的der和pem编码格式比较](#)

[Chen-PKI系统与数字证书结构](#)

作者: [zale](#)

出处: <http://www.cnblogs.com/littleatp/>, 如果喜欢我的文章, 请关注我的公众号



本文版权归作者和博客园共有，欢迎转载，但未经作者同意必须保留此段声明，且在文章页面明显位置给出 [原文链接](#) 如有问题，可留言咨询。

分类: [2.安全技术](#)


标签: [安全技术](#), [公钥证书](#)

« 上一篇: [使用H2数据库进行单元测试](#)

» 下一篇: [mongodb 认证鉴权那点事](#)

posted @ 2017-08-17 22:21 美码师 阅读(3279) 评论(0) 编辑 收藏

[刷新评论](#) [刷新页面](#) [返回顶部](#)

 注册用户登录后才能发表评论，请 [登录](#) 或 [注册](#)，[访问网站首页](#)。

【推荐】超50万C++/C#源码：大型实时仿真组态图形源码

【前端】SpreadJS表格控件，可嵌入系统开发的在线Excel

【推荐】从Java菜鸟到大牛的成长秘籍

【推荐】程序员问答平台，解决您开发中遇到的技术难题

相关博文：

- [公钥证书编码解读](#)
- [Atitti.数字证书体系cer pfx attilax总结](#)
- [Atitti.数字证书体系cer pfx attilax总结](#)
- [数字证书常见格式整理](#)
- [常见证书格式和转换](#)

最新新闻：

- [天文学家称月球最大的陨石坑下方隐藏着神秘物质](#)
 - [可循环利用食品包装透明薄膜问世](#)
 - [亚马逊成全球最具价值品牌 阿里腾讯进前10强](#)
 - [学问经得起时间考验的傅立叶](#)
 - [美司法部警告科技巨头：没商业意义的收购视为垄断](#)
- » [更多新闻...](#)



Copyright ©2019 美码师