An example of X.509 and it's operational principle

13331233 孙中阳

X.509

X.509被广泛使用的数字证书标准，是由国际电联电信委员会（ITU-T）为单点登录（SSO-Single Sign-on）和授权管理基础设施（PMI-Privilege Management Infrastructure）制定的PKI标准，发布于1988年7月3日。

单点登录

单点登录（Single Sign On），简称为 SSO，是目前比较流行的企业业务整合的解决方案之一。SSO的定义是在多个应用系统中，用户只需要登录一次就可以访问所有相互信任的应用系统。

授权管理基础设施PMI

向用户和应用程序提供授权管理服务，提供用户身份到应用授权的映射功能，提供与实际应用处理模式相对应的、与具体应用系统开发和管理无关的授权和访问控制机制，简化具体应用系统的开发与维护。

PMI和PKI

PKI证明用户是谁，而PMI证明这个用户有什么权限，能干什么，授权管理基础设施PMI根据公钥基础设施PKI为用户提供身份认证。

Principle

1. 基本结构

1.1. 版本号. 标识证书的版本（版本1、版本2或是版本3）

1.2. 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

1.3. 签名 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和RSA的对象标识符就用来说明该数字签名是利用RSA对SHA-1杂凑加密

1.4. 颁发者 证书颁发者的可识别名（DN）

1.5. 有效期 证书有效期的时间段。本字段由”Not Before”和”Not After”两项组成，它们分别由UTC时间或一般的时间表示（在RFC2459中有详细的时间表示规则）

1.6. 主体 证书拥有者的可识别名，这个字段必须是非空的，除非你在证书扩展中有别名

1.7. 主体公钥信息 主体的公钥（以及算法标识符）

1.8. 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

1.9. 主体唯一标识符 证书拥有者的唯一标识符，仅在版本2和版本3中有要求，属于可选项

2. 工作流程

来自 x509-百度百科

1.从磁盘上的证书文件中读取证书数据

```
    unsigned char* pbX509Data; // 证书数据
    unsigned long ulX509DataLen; // 证书数据长度
```

2.获取CertContext

```
    PCCERT_CONTEXT pCertContext = CertCreateCertificateConte
xt(X509_ASN_ENCODING, pbX509Data, ulX509DataLen);
```

3.获取证书信息

```
   pCertContext->pCertInfo->dwVersion; // 证书版本号
   CRYPT_INTEGER_BLOB snBlob = pCertContext->pCertInfo->Ser
ialNumber; // 证书SN
   CERT_NAME_BLOB issuerBlob = pCertContext->pCertInfo->Iss
uer; // 证书颁发者
   CERT_NAME_BLOB subjectBlob = pCertContext->pCertInfo->Su
bject; // 证书主题
   // 证书有效起始日期
   SYSTEMTIME sysTime;
   memset(&sysTime, 0, sizeof(sysTime));
   FileTimeToSystemTime(&pCertContext->pCertInfo->NotBefore
, &sysTime);
   char szTime[128] = {0};
   sprintf_s(szTime, 128, "%d年%d月%d日 %d:%d:%d", sysTime.w
Year, sysTime.wMonth, sysTime.wDay, sysTime.wHour, sysTime.
wMinute, sysTime.wSecond);
   // 证书有效终止日期
   memset(&sysTime, 0, sizeof(sysTime));
   FileTimeToSystemTime(&pCertContext->pCertInfo->NotAfter,
 &sysTime);
   memset(szTime, 0, sizeof(szTime));
   sprintf_s(szTime, 128, "%d年%d月%d日 %d:%d:%d", sysTime.w
Year, sysTime.wMonth, sysTime.wDay, sysTime.wHour, sysTime.
wMinute, sysTime.wSecond);
```

4.创建临时密钥容器

```
   HCRYPTPROV hTmpProv = NULL;
   CryptAcquireContext(&hTmpProv, "My_Temporary_Container",
 NULL, PROV_RSA_AES, 0); // NULL表示使用系统默认CSP
```

5.向容器中导入公钥，获取公钥句柄

```
   HCRYPTKEY hKey = NULL;
   CERT_PUBLIC_KEY_INFO certPubKeyInfo = pCertContext->pCer
tInfo->SubjectPublicKeyInfo;
   CryptImportPublicKeyInfo(hTmpProv, X509_ASN_ENCODING|PKC
S_7_ASN_ENCODING, &certPubKeyInfo, &hKey);
```

6.导出公钥（最好采用二次调用方式）

```
    unsigned char* pBuf = NULL;
    unsigned long ulBufLen = 0;
    CryptExportKey(hKey, 0, PUBLICKEYBLOB, 0, pBuf, &ulBufLe
n);
    pBuf = new unsigned char[ulBufLen];
    memset(pBuf, 0, ulBufLen);
    CryptExportKey(hKey, 0, PUBLICKEYBLOB, 0, pBuf, &ulBufLe
n);
```

7.获取公钥信息

```
    unsigned char* p = pBuf + sizeof(PUBLICKEYSTRUC);
    (*(RSAPUBKEY*)p).bitlen; // 公钥模长（以bit为单位）
    (*(RSAPUBKEY*)p).pubexp; // 公钥的e（注意字节顺序）
    p += sizeof(RSAPUBKEY); // 公钥的n（注意字节顺序）
```

8.清理工作

```
    delete[] pBuf;
    pBuf = NULL;
    CryptDestroyKey(hKey);
    CryptReleaseContext(hTmpProv, 0);
    CertFreeCertificateContext(pCertContext);
```

Example

来自 Focus on biztalk -- chnking 的实例

DSA证书，CA证书

证书包含699字节，证书版本号为3

```
(a) 证书序列号是17 (0x11);
(b) 证书使用DSA和SHA-1哈希算法签名;
(c) 证书发行者的名字是OU=nist; O=gov; C=US
(d) 证书主体的名字是OU=nist; O=gov; C=US
(e) 证书的有效期从1997-6-30到 1997-12-31;
(f) 证书包含一个1024 bit DSA 公钥及其参数（三个整数p、q、g）;
(g) 证书包含一个使用者密钥标识符(subjectKeyIdentifier)扩展项
(h) 证书是一个CA证书(通过basicConstraints基本扩展项标识)
```

该证书包含以下内容：

```
   0000 30 82 02 b7 695: SEQUENCE    // Certificate:: SEQUE
NCE类型(30)，数据块长度字节
   为2（82），长度为695（02 b7）
   0004 30 82 02 77 631: . SEQUENCE // tbsCertificate:: SEQ
UENCE类型,长度631
   0008 a0 03          3: . . [0]     // Version:: 特殊内容-
证书版本(a0),长度3
   0010 02 01          1: . . . INTEGER 2 //整数类型(02),长度
1
                        : 02               // 版本3(2)
   0013 02 01          1: . . INTEGER 17   // serialNumber:
: 整数类型(02),长度1
                        : 11               // 证书序列号 17
   0016 30 09          9: . . SEQUENCE   // signature:: SEQ
UENCE类型(30),长度9
   0018 06 07          7: . . . OID 1.2.840.10040.4.3: dsa-
with-sha //signature:: OBJECT

   IDENTIFIER类型,长度7
                        : 2a 86 48 ce 38 04 03   // 表示dsa-
with-sha算法(见注1)
   0027 30 2a         42: . . SEQUENCE            // 以下红
色的数据块表示issuer信息
   0029 31 0b         11: . . . SET
   0031 30 09          9: . . . . SEQUENCE
   0033 06 03          3: . . . . . OID 2.5.4.6: C
                        : 55 04 06
   0038 13 02          2: . . . . . PrintableString 'US'
                        : 55 53
   0042 31 0c         12: . . . SET
   0044 30 0a         10: . . . . SEQUENCE
```

```
   0046 06 03          3: . . . . . OID 2.5.4.10: O
                        : 55 04 0a
   0051 13 03          3: . . . . . PrintableString 'gov'
                        : 67 6f 76
   0056 31 0d         13: . . . SET
   0058 30 0b         11: . . . . SEQUENCE
   0060 06 03          3: . . . . . OID 2.5.4.11: OU
                        : 55 04 0b
   0065 13 04          4: . . . . . PrintableString 'nist'
                        : 6e 69 73 74
   0071 30 1e         30: . . SEQUENCE         // validity:
: SEQUENCE类型(30),长度30
   0073 17 0d         13: . . . UTCTime '970630000000Z' //
notBefore:: UTCTime类型(23)

   长度13
                        : 39 37 30 36 33 30 30 30 30 30 30
30 5a
   0088 17 0d         13: . . . UTCTime '971231000000Z' //
notBefore:: UTCTime类型(23)

   长度13
                        : 39 37 31 32 33 31 30 30 30 30 30
30 5a
   0103 30 2a         42: . . SEQUENCE          // 以下红色的
数据块表示subject信息
   0105 31 0b         11: . . . SET
   0107 30 09          9: . . . . SEQUENCE
   0109 06 03          3: . . . . . OID 2.5.4.6: C
                        : 55 04 06
   0114 13 02          2: . . . . . PrintableString 'US'
                        : 55 53
   0118 31 0c         12: . . . SET
   0120 30 0a         10: . . . . SEQUENCE
   0122 06 03          3: . . . . . OID 2.5.4.10: O
                        : 55 04 0a
   0127 13 03          3: . . . . . PrintableString 'gov'
                        : 67 6f 76
   0132 31 0d         13: . . . SET
   0134 30 0b         11: . . . . SEQUENCE
   0136 06 03          3: . . . . . OID 2.5.4.11: OU
                        : 55 04 0b
   0141 13 04          4: . . . . . PrintableString 'nist'
```

```
                        : 6e 69 73 74
   0147 30 82 01 b4 436: . . SEQUENCE // subjectPublicKeyIn
fo:: SEQUENCE类型(30),

   长度436
   0151 30 82 01 29 297: . . . SEQUENCE
   0155 06 07          7: . . . . OID 1.2.840.10040.4.1: ds
a //algorithm:: OBJECT

   IDENTIFIER类型,长度7
                        : 2a 86 48 ce 38 04 01    // 表示DSA
算法(见注1)
   0164 30 82 01 1c 284: . . . . SEQUENCE        // DSA算法
的parameters,三个整数

   p、q、g
   0168 02 81 80     128: . . . . . INTEGER       // p参数
                        : d4 38 02 c5 35 7b d5 0b a1 7e 5d
72 59 63 55 d3
                        : 45 56 ea e2 25 1a 6b c5 a4 ab aa
0b d4 62 b4 d2
                        : 21 b1 95 a2 c6 01 c9 c3 fa 01 6f
79 86 83 3d 03
                        : 61 e1 f1 92 ac bc 03 4e 89 a3 c9
53 4a f7 e2 a6
                        : 48 cf 42 1e 21 b1 5c 2b 3a 7f ba
be 6b 5a f7 0a
                        : 26 d8 8e 1b eb ec bf 1e 5a 3f 45
c0 bd 31 23 be
                       : 69 71 a7 c2 90 fe a5 d6 80 b5 24 d
c 44 9c eb 4d
                        : f9 da f0 c8 e8 a2 4c 99 07 5c 8e
35 2b 7d 57 8d
   0299 02 14         20: . . . . . INTEGER       // q参数
                        : a7 83 9b f3 bd 2c 20 07 fc 4c e7
e8 9f f3 39 83
                        : 51 0d dc dd
   0321 02 81 80     128: . . . . . INTEGER       // g参数
                        : 0e 3b 46 31 8a 0a 58 86 40 84 e3
a1 22 0d 88 ca
                        : 90 88 57 64 9f 01 21 e0 15 05 94
24 82 e2 10 90
                        : d9 e1 4e 10 5c e7 54 6b d4 0c 2b
```

```
1b 59 0a a0 b5
                        : a1 7d b5 07 e3 65 7c ea 90 d8 8e
30 42 e4 85 bb
                        : ac fa 4e 76 4b 78 0e df 6c e5 a6
e1 bd 59 77 7d
                        : a6 97 59 c5 29 a7 b3 3f 95 3e 9d
f1 59 2d f7 42
                        : 87 62 3f f1 b8 6f c7 3d 4b b8 8d
74 c4 ca 44 90
                        : cf 67 db de 14 60 97 4a d1 f7 6d
9e 09 94 c4 0d
   0452 03 81 84     132: . . . BIT STRING (0 unused bits)
// subjectPublicKey::

   公钥值，BIT STRING类型，长度132字节(好像应该是131字节)
   0455 02 81 80     128: . . . . INTEGER // 公钥值，表现为in
teger类型,128字节,1024位
   : aa 98 ea 13 94 a2 db f1 5b 7f 98 2f 78 e7 d8 e3
                        : b9 71 86 f6 80 2f 40 39 c3 da 3b
4b 13 46 26 ee
                        : 0d 56 c5 a3 3a 39 b7 7d 33 c2 6b
5c 77 92 f2 55
                        : 65 90 39 cd 1a 3c 86 e1 32 eb 25
bc 91 c4 ff 80
                        : 4f 36 61 bd cc e2 61 04 e0 7e 60
13 ca c0 9c dd
                        : e0 ea 41 de 33 c1 f1 44 a9 bc 71
de cf 59 d4 6e
                        : da 44 99 3c 21 64 e4 78 54 9d d0
7b ba 4e f5 18
                        : 4d 5e 39 30 bf e0 d1 f6 f4 83 25
4f 14 aa 71 e1
   0587 a3 32         50: . . [3]             // extensions
:: 特殊内容-证书扩展部分(a3),

   长度50
   0589 30 30         48: . . . SEQUENCE
   0591 30 0f          9: . . . . SEQUENCE   // 扩展basicCon
straints
   0593 06 03          3: . . . . . OID 2.5.29.19: basicCon
straints
                        : 55 1d 13
   0598 01 01          1: . . . . . TRUE     // true，表示为
```

```
CA证书
                          : ff
   0601 04 05           5: . . . . . OCTET STRING
                          : 30 03 01 01 ff
   0608 30 1d          29: . . . . SEQUENCE   // 扩展 subject
KeyIdentifier
   0610 06 03           3: . . . . . OID 2.5.29.14: subjectK
eyIdentifier
                          : 55 1d 0e
   0615 04 16          22: . . . . . OCTET STRING //扩展 subj
ectKeyIdentifier的值
                          : 04 14 e7 26 c5 54 cd 5b a3 6f 35
68 95 aa d5 ff
                          : 1c 21 e4 22 75 d6
   0639 30 09           9: . SEQUENCE // signatureAlgorithm:
: = AlgorithmIdentifier
   0641 06 07           7: . . OID 1.2.840.10040.4.3: dsa-wi
th-sha
                          : 2a 86 48 ce 38 04 03
   0650 03 2f          47: . BIT STRING (0 unused bits) // b
it串，证书签名值，47字节
   0652 30 2c          44: . . SEQUENCE
   0654 02 14          20: . . . INTEGER       // 签名值,20字
节,160bit
                          : a0 66 c1 76 33 99 13 51 8d 93 64
2f ca 13 73 de
                          : 79 1a 7d 33
   0674 02 14          20: . . . INTEGER       // 签名值,20字
节,160bit
   : 5d 90 f6 ce 92 4a bf 29 11 24 80 28 a6 5a 8e 73
                          : b6 76 02 68
```