

## X.509 数字证书结构和实例

### 一、X.509数字证书的编码

X.509证书的结构是用ASN1(Abstract Syntax Notation One)进行描述数据结构，并使用ASN1语法进行编码。

ASN1采用一个个的数据块来描述整个数据结构，每个数据块都有四个部分组成：

#### 1、数据块数据类型标识（一个字节）

数据类型包括简单类型和结构类型。

简单类型是不能再分解类型，如整型(INTEGER)、比特串(BIT STRING)、字节串(OCTET STRING)、对象标识符(OBJECT IDENTIFIER)、日期型(UTCTime)等。

结构类型是由简单类型和结构类型组合而成的，如顺序类型(SEQUENCE, SEQUENCE OF)、选择类型(CHOICE)、集合类型(SET)等。

- 顺序类型的数据块值由按给定顺序成员成员数据块值按照顺序组成，；
- 选择类型的数据块值由多个成员数据数据块类型中选择一个的数据块值；
- 集合数据块类型由成员数据块类型的一个或多个值构成。

这个标识字节的结构如下：

#### 1.1. Bit8-bit7

用来标示 TAG 类型，共有四种，分别是universal(00)、application(01)、context-specific(10)和private(11)。

这两位为universal（00）时，bit5-bit1的值表示不同的universal的值：

标记（TAG）      对应类型

[UNIVERSAL 1] BOOLEAN [有两个值:false或true]

[UNIVERSAL 2] INTEGER [整型值]

[UNIVERSAL 3] BIT STRING [0位或多位]

[UNIVERSAL 4] OCTET STRING [0字节或多字节]

[UNIVERSAL 5] NULL

[UNIVERSAL 6] OBJECT IDENTIFIER [相应于一个对象的独特标识数字]

[UNIVERSAL 7] OBJECT DESCRIPTOR [一个对象的简称]

[UNIVERSAL 8] EXTERNAL, INSTANCE OF [ASN.1没有定义的数据类型]

[UNIVERSAL 9] REAL [实数值]

[UNIVERSAL 10] ENUMERATED [数值列表，这些数据每个都有独特的标识符，作为ASN.1定义数据类型的一部分]

[UNIVERSAL 12] UTF8String

[UNIVERSAL 13] RELATIVE-OID

**[UNIVERSAL 16] SEQUENCE, SEQUENCE OF** [有序数列，**SEQUENCE**里面的每个数值都可以是不同类型的，而**SEQUENCE OF**里是0个或多个类型相同的数据]

**[UNIVERSAL 17] SET, SET OF** [无序数列，**SET**里面的每个数值都可以是不同类型的，而**SET OF**里是0个或多个类型相同的数据]

[UNIVERSAL 18] NumericString [0-9以及空格]

[UNIVERSAL 19] PrintableString [A-Z、a-z、0-9、空格以及符号'()+,-./:=?]

[UNIVERSAL 20] TeletexString, T61String

[UNIVERSAL 21] VideotexString

[UNIVERSAL 22] IA5String

[UNIVERSAL 23] UTCTime [统一全球时间格式]

[UNIVERSAL 24] GeneralizedTime

[UNIVERSAL 25] GraphicString

[UNIVERSAL 26] VisibleString, ISO646String

[UNIVERSAL 27] GeneralString

[UNIVERSAL 28] UniversalString

[UNIVERSAL 29] CHARACTER STRING

[UNIVERSAL 30] BMPString

[UNIVERSAL 31]... reserved for future use

这两位为context-specific（10）时，bit5-bit1的值表示特殊内容：

[0] -- 表示证书的版本

[1] -- issuerUniqueID,表示证书发行者的唯一id

[2] -- subjectUniqueID,表示证书主体的唯一id

[3] -- 表示证书的扩展字段

## 1.2. bit6

表示是否为结构类型(1位结构类型)；0则表明编码类型是简单类型。

### 1.3. bit5-bit1

是类型的TAG值。根据bit8-bit7的不同值有不同的含义，具体含义见上面的描述。

如 SEQUENCE 类型数据块，其TAG类型位UNIVERSAL (00) ,属于结构类型 (1) , TAG值为16 (10000) 所以其类型标示字段值为 (00110000) , 即为0x30。

再如，证书扩展字段类型的数据块，TAG类型为 (10) , 属结构类型 (1) , TAG的值为3 (00011) , 所以其类型标示字段值为 (10100011) , 即为0xA3。

## 2、数据块长度 ( 1-128个字节 )

长度字段，有两种编码格式。

若长度值小于等于127，则用一个字节表示，bit8 = 0, bit7-bit1 存放长度值；

若长度值大于127，则用多个字节表示，可以有2到127个字节。第一个字节的第8位为1，其它低7位给出后面该域使用的字节的数量，从该域第二个字节开始给出数据的长度，高位优先。

还有一种特殊情况，这个字节为0x80，表示数据块长度不定，由数据块结束标识结束数据块。

## 3、数据块的值

存放数据块的值，具体编码随数据块类型不同而不同。

## 4、数据块结束标识 ( 可选 )

结束标示字段，两个字节 (0x0000) ,只有在长度值为不定时才会出现。

## 二、 X.509证书的结构

### 1、X.509证书基本部分

#### 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、X.509证书扩展部分

可选的标准和专用的扩展（仅在版本2和版本3中使用），扩展部分的元素都有这样的结构：

```
Extension ::= SEQUENCE {  
    extnID      OBJECT IDENTIFIER,  
    critical    BOOLEAN DEFAULT FALSE,  
    extnValue   OCTET STRING }
```

extnID: 表示一个扩展元素的OID

critical: 表示这个扩展元素是否极重要

extnValue: 表示这个扩展元素的值，字符串类型。

扩展部分包括：

## 2.1. 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。

## 2.2. 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署证书，而不应该用于SSL。

## 2.3. CRL分布点

指明CRL的分布地点。

2.4. 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。

2.5. 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。

2.6. 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。

2.7. 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。

2.8. 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。

2.9. 主体目录属性

指出证书拥有者的一系列属性。可以使用这一项来传递访问控制信息。

三、X.509证书详细描述

```
Certificate ::= SEQUENCE {
    tbsCertificate      TBSCertificate, -- 证书主体
    signatureAlgorithm  AlgorithmIdentifier, -- 证书签名算法标识
    signatureValue      BIT STRING --证书签名值,是使用
                                   signatureAlgorithm部分指定的签名算法对
                                   tbsCertificate证书主题部分签名后的值.
}

TBSCertificate ::= SEQUENCE {
    version             [0] EXPLICIT Version DEFAULT v1, -- 证书版本号
    serialNumber        CertificateSerialNumber, -- 证书序列号,对同一CA所颁发的证书,序列号唯一标识证书
    signature           AlgorithmIdentifier, --证书签名算法标识
    issuer              Name, --证书发行者名称
```

```

        validity          Validity,          --证书有
有效期
        subject           Name,              --证书主
主体名称
        subjectPublicKeyInfo SubjectPublicKeyInfo, --证书公
钥
        issuerUniqueID [1] IMPLICIT UniqueIdentifier
OPTIONAL,
                                -- 证书发行者ID(可选), 只在证书
版本2、3中才有
        subjectUniqueID [2] IMPLICIT UniqueIdentifier
OPTIONAL,
                                -- 证书主体ID(可选), 只在证书版
本2、3中才有
        extensions       [3] EXPLICIT Extensions OPTIONAL
                                -- 证书扩展段(可选), 只在证书
版本3中才有
    }
    Version ::= INTEGER { v1(0), v2(1), v3(2) }
    CertificateSerialNumber ::= INTEGER

    AlgorithmIdentifier ::= SEQUENCE {
        algorithm          OBJECT IDENTIFIER,
        parameters         ANY DEFINED BY algorithm
OPTIONAL }
    parameters:
    Dss-Parms ::= SEQUENCE { -- parameters , DSA(DSS)算法时的parameters,
                                RSA算法没有此参数

        p                INTEGER,
        q                INTEGER,
        g                INTEGER }

    signatureValue:
    Dss-Sig-Value ::= SEQUENCE { -- sha1DSA签名算法时, 签名值
        r                INTEGER,
        s                INTEGER }

    Name ::= CHOICE {
        RDNSequence }
    RDNSequence ::= SEQUENCE OF RelativeDistinguishedName
    RelativeDistinguishedName ::=
        SET OF AttributeTypeAndValue
    AttributeTypeAndValue ::= SEQUENCE {
        type      AttributeType,
        value     AttributeValue }
    AttributeType ::= OBJECT IDENTIFIER
    AttributeValue ::= ANY DEFINED BY AttributeType

```

```

Validity ::= SEQUENCE {
    notBefore      Time, -- 证书有效期起始时间
    notAfter       Time -- 证书有效期终止时间
}
Time ::= CHOICE {
    utcTime        UTCTime,
    generalTime    GeneralizedTime }
UniqueIdentifier ::= BIT STRING
SubjectPublicKeyInfo ::= SEQUENCE {
    algorithm       AlgorithmIdentifier, -- 公钥算
法
    subjectPublicKey BIT STRING          -- 公钥
值
}
subjectPublicKey:
RSAPublicKey ::= SEQUENCE { -- RSA算法时的公钥值
    modulus          INTEGER, -- n
    publicExponent   INTEGER -- e -- }

Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension
Extension ::= SEQUENCE {
    extnID          OBJECT IDENTIFIER,
    critical        BOOLEAN DEFAULT FALSE,
    extnValue       OCTET STRING }

```

#### 四、X.509数字证书实例

这是从RFC 2459 Internet X.509 Public Key Infrastructure标准文档中摘取的两个证书例子。本文在例子的原来基础上加了些注释。

##### 1、DSA证书, CA证书

证书包含699字节, 证书版本号为3。

该证书包含以下内容:

- (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)

```

0000 30 82 02 b7 695: SEQUENCE // Certificate:: SEQUENCE
                                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::
SEQUENCE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::
SEQUENCE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

```



```

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: 0
                                                         : 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 //
                                                         subjectPublicKeyInfo::
                                                         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:
                                                         dsa //algori
                                                         thm::
                                                         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 dc
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
integer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
basicConstraints
0593 06 03      3: . . . . . OID 2.5.29.19:
basicConstraints
                                : 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
subjectKeyIdentifier
0610 06 03      3: . . . . . OID 2.5.29.14:
subjectKeyIdentifier
                                : 55 1d 0e
0615 04 16      22: . . . . . OCTET STRING //扩展
subjectKeyIdentifier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-with-
sha
                                : 2a 86 48 ce 38 04 03
0650 03 2f      47: . BIT STRING (0 unused bits) // bit
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

```

## 2、RSA证书，非CA证书

证书包含675字节，证书版本号为3。

该证书包含以下内容：

- (a) 证书序列号是256 (0x100);
- (b) 证书使用RSA和MD2哈希算法签名;
- (c) 证书发行者的名字是OU=Dept. Arquitectura de Computadors; O=Universitat Politecnica de Catalunya; C=ES
- (d) 证书主体的名字是CN=Francisco Jordan;OU=Dept. Arquitectura de Computadors; O=Universitat Politecnica de Catalunya; C=ES
- (e) 证书的有效期从1996-5-21到 1997-5-21;
- (f) 证书包含一个768 bit RSA 公钥;
- (g) 证书是一个非CA证书(通过一个基本扩展项标识)
- (h) 证书包含证书主体别名、证书发行者别名-都是URLs
- (i) 证书包含一个发行者密钥标识符和证书策略扩展，和
- (j) 证书包含一个密钥用法的扩展，指定用于数字签名

```

0000 30 80          : SEQUENCE      (size undefined) //
                                                    Certificate:
                                                    : SEQUENCE类
                                                    型(30)，数据
                                                    块长度不定，
                                                    由00、00作为
                                                    结束符

0002 30 82 02 40 576: . SEQUENCE      // tbsCertificate::
SEQUENCE类型,长度576

0006 a0 03          3: . . [0]        // Version:: 特殊
内容-证书版本(a0),长度3

0008 02 01          1: . . . INTEGER 2 //整数类型(02),长度
1
                                     : 02          // 版本3(2)

0011 02 02          2: . . INTEGER 256 //serialNumber::
整数类型(02),长度2
                                     : 01 00        // 证书序列号256

0015 30 0d          13: . . . SEQUENCE // signature::
SEQUENCE类型(30),长度13

0017 06 09          9: . . . OID 1.2.840.113549.1.1.2:
MD2WithRSAEncryption
                                                    // signature:: OBJECT
                                                    IDENTIFIER类
                                                    型,长度9
                                     : 2a 86 48 86 f7 0d 01 01 02
//MD2WithRSAEncryption算法(见注1)

0028 05 00          0: . . . NULL

```

```

0030 30 68      88: . . SEQUENCE           // 以下红
色的数据块表示issuer信息
0032 31 0b      11: . . . SET
0034 30 09      9: . . . . SEQUENCE
0036 06 03      3: . . . . . OID 2.5.4.6: C
                  : 55 04 06
0041 13 02      2: . . . . . PrintableString 'ES'
                  : 45 53
0045 31 2d      45: . . . SET
0047 30 2b      43: . . . . SEQUENCE
0049 06 03      3: . . . . . OID 2.5.4.10: 0
                  : 55 04 0a
0054 13 24      36: . . . . . PrintableString
                  'Universitat Politecnica de Catalunya'
                  : 55 6e 69 76 65 72 73 69 74 61 74 20
50 6f 6c 69
                  : 74 65 63 6e 69 63 61 20 64 65 20 43
61 74 61 6c
                  : 75 6e 79 61
0092 31 2a      42: . . . SET
0094 30 28      40: . . . . SEQUENCE
0096 06 03      3: . . . . . OID 2.5.4.11: OU
                  : 55 04 0b
0101 13 21      33: . . . . . PrintableString
                  'OU=Dept. Arquitectura de Computadors'
                  : 44 65 70 74 2e 20 41 72 71 75 69 74
65 63 74 75
                  : 72 61 20 64 65 20 43 6f 6d 70 75 74
61 64 6f 72
                  : 73
0136 30 1e      30: . . SEQUENCE           // validity::
SEQUENCE类型(30),长度30
0138 17 0d      13: . . . UTCTime '960521095826Z' //
notBefo
re::
UTCTime
类型
(23)

长度13
: 39 36 30 37 32 32 31 37 33 38 30 32
5a
0153 17 0d      13: . . . UTCTime '979521095826Z' //
notBefo
re::
UTCTime
类型
(23)

长度13

```

: 39 37 30 37 32 32 31 37 33 38 30 32

5a

0168 30 81 83 112: . . SEQUENCE // 以下红色的数据块表示subject信息

0171 31 0b 11: . . . SET

0173 30 09 9: . . . . SEQUENCE

0175 06 03 3: . . . . . OID 2.5.4.6: C  
: 55 04 06

0180 13 02 2: . . . . . PrintableString 'ES'  
: 45 53

0184 31 2d 12: . . . SET

0186 30 2b 16: . . . . SEQUENCE

0188 06 03 3: . . . . . OID 2.5.4.10: 0  
: 55 04 0a

0193 13 24 36: . . . . . PrintableString  
'Universitat Politecnica de Catalunya'  
: 55 6e 69 76 65 72 73 69 74 61 74 20

50 6f 6c 69 : 74 65 63 6e 69 63 61 20 64 65 20 43

61 74 61 6c : 75 6e 79 61

0231 31 2a 42: . . . SET

0233 30 28 40: . . . . SEQUENCE

0235 06 03 3: . . . . . OID 2.5.4.11: OU  
: 55 04 0b

0240 13 21 33: . . . . . PrintableString  
'Dept. Arquitectura de Computadors'  
: 44 65 70 74 2e 20 41 72 71 75 69 74

65 63 74 75 : 72 61 20 64 65 20 43 6f 6d 70 75 74

61 64 6f 72 : 73

0275 31 19 22: . . . SET

0277 30 17 20: . . . . SEQUENCE

0279 06 03 3: . . . . . OID 2.5.4.3: CN  
: 55 04 03

0284 13 10 16: . . . . . PrintableString 'Francisco  
Jordan'  
: 46 72 61 6e 63 69 73 63 6f 20 4a 6f

72 64 61 6e

0302 30 7c 2: . . SEQUENCE //  
subjectPublicKeyInfo::  
SEQUENCE类型(30),

长度不定

0304 30 0d 13: . . . SEQUENCE

0306 06 09 9: . . . . . OID 1.2.840.113549.1.1.1:  
RSAEncryption  
//algorithm::

```

OBJECT
IDENTIFIER类型,
长度9
: 2a 86 48 86 f7 0d 01 01 01 // 表示
RSA算法(见注1)
0317 05 00      0: . . . . NULL
0319 03 6b      107: . . . BIT STRING (0 unused bits) //
subjectPublicKey
::

公钥值, BIT
STRING类型, 长度
107字节

: 00 (0 unused bits)
0321 03 68      104: . . . . BIT STRING (0 unused bits)
0323 02 61      97: . . . . . INTEGER (0 unused bits)
// 公钥值, 96字节, 768位
: 00 (0 unused bits)
: be aa 8b 77 54 a3 af ca 77 9f 2f b0
cf 43 88 ff
: a6 6d 79 55 5b 61 8c 68 ec 48 1e 8a
86 38 a4 fe
: 19 b8 62 17 1d 9d 0f 47 2c ff 63 8f
29 91 04 d1
: 52 bc 7f 67 b6 b2 8f 74 55 c1 33 21
6c 8f ab 01
: 95 24 c8 b2 73 93 9d 22 61 50 a9 35
fb 9d 57 50
: 32 ef 56 52 50 93 ab b1 88 94 78 56
15 c6 1c 8b
0423 02 03      3: . . . . . INTEGER // RSA加密算法的
exponent值
: 01 00 01
0428 a3 81 97   151: . . [3] // extensions:: 特殊
内容-证书扩展部分(a3),

长度151
0431 30 3c      60: . . . SEQUENCE
0433 30 1f      31: . . . . SEQUENCE // 扩展发行
者密钥标识符

authorityKeyI
dentifier
0435 06 03      3: . . . . . OID 2.5.29.35:
authorityKeyIdentifier
: 55 1d 23
0440 04 14      22: . . . . . OCTET STRING
: 30 12 80 10 0e 6b 3a bf 04 ea 04 c3
0e 6b 3a bf
: 04 ea 04 c3

```

```

0464 30 19      25: . . . . SEQUENCE      // 扩展
keyUsage
0466 06 03      3: . . . . . OID 2.5.29.15: keyUsage
                  : 55 1d 0f
0471 01 01      1: . . . . . TRUE
                  : ff
0474 04 04      4: . . . . . OCTET STRING
                  : 03 02 07 80
0480 30 19      25: . . . . SEQUENCE      //扩展
certificatePolicies
0482 06 03      3: . . . . . OID 2.5.29.32:
certificatePolicies
                  : 55 1d 20
0487 04 21      33: . . . . . OCTET STRING
                  : 30 1f 30 1d 06 04 2a 84 80 00 30 15
30 07 06 05
                  : 2a 84 80 00 01 30 0a 06 05 2a 84 80
00 02 02 01
                  : 0a
0522 30 1c      28: . . . . SEQUENCE      //扩展
subjectAltName
0524 06 03      3: . . . . . OID 2.5.29.17:
subjectAltName
                  : 55 1d 11
0529 04 15      21: . . . . . OCTET STRING
                  : 30 13 86 11 68 74 74 70 3a 2f 2f 61
63 2e 75 70
                  : 63 2e 65 73 2f
0552 30 19      25: . . . . SEQUENCE      //扩展
issuerAltName
0554 06 03      3: . . . . . OID 2.5.29.18:
issuerAltName
                  : 55 1d 12
0559 04 12      18: . . . . . OCTET STRING
                  : 30 14 86 12 68 74 74 70 3a 2f 2f 77
77 77 2e 75
                  : 70 63 2e 65
0579 30 80      : . SEQUENCE (indefinite length) //
signatu
reAlgor
ithm

不知为何
这里的前
面算法为
空

0581 06 07      7: . . OID
0583 05 00      0: . . NULL
0585 00 00      0: . . end of contents marker
0587 03 81 81   47: . BIT STRING      // 签名值

```



```

: 00      (0 unused bits)
: 5c 01 bd b5 41 88 87 7a 0e d3 0e 6b
3a bf 04 ea
: 04 cb 5f 61 72 3c a3 bd 78 f5 66 17
fe 37 3a ab
: eb 67 bf b7 da a8 38 f6 33 15 71 75
2f b9 8c 91
: a0 e4 87 ba 4b 43 a0 22 8f d3 a9 86
43 89 e6 50
: 5c 01 bd b5 41 88 87 7a 0e d3 0e 6b
3a bf 04 ea
: 04 cb 5f 61 72 3c a3 bd 78 f5 66 17
fe 37 3a ab
: eb 67 bf b7 da a8 38 f6 33 15 71 75
2f b9 8c 91
: a0 e4 87 ba 4b 43 a0 22 8f d3 a9 86
43 89 e6 50
0637 00 00      0: . . end of contents marker

```

注1: OID表示的算法

```

DSA -- 1.2.840.10040.4.1
sha1DSA -- 1.2.840.10040.4.3
RSA -- 1.2.840.113549.1.1.1
md2RSA -- 1.2.840.113549.1.1.2
md4RSA -- 1.2.840.113549.1.1.3
md5RSA -- 1.2.840.113549.1.1.4
sha1RSA -- 1.2.840.113549.1.1.5

```

参考:

[RFC 2459 Internet X.509 Public Key Infrastructure](#)

[X.509证书结构简介及实例](#)

[X.509第三版的证书结构](#)

分类: [4.其他技术区](#),[VS2005&C#](#),[biztalk](#)

好文要顶

关注我

收藏该文



chnking

关注 - 0

粉丝 - 147

[+加关注](#)

4

0

« 上一篇: [使用X.509数字证书加密解密实务 \(一\) -- 证书的获得和管理](#)

» 下一篇: [使用X.509数字证书加密解密实务 \(二\) -- 使用RSA证书加密敏感数据](#)

posted on 2007-08-28 00:32 [chnking](#) 阅读(29351) 评论(4) [编辑](#) [收藏](#)

## 评论

### #1楼 2008-04-09 00:02 蓝奇高级验证码识别引擎QQ:631753663

出售蓝奇高级验证码识别引擎，可准确识别新浪网淘宝CSDN等多种复杂验证码。

输出为一个标准DLL，可供VB,VC,Delphi,C#.NET,VB.NET,模拟精灵,按键精灵等多平台调用，调用方法简单，几行代码即可完成。独具特色的边缘检测字符分离、旋转倾斜纠正和通用字符匹配算法（无论字体和大小），使得该引擎对于像新浪、动网、淘宝、CSDN等多种验证码均有不错的识别率，是一款效果较为理想的验证码识别引擎。附详细的调用实例和代码注释等相关技术文档。

官方网站 - [http://\\*\\*\\*/yzm\\_advocr](http://***/yzm_advocr)

识别效果怎么样一试就知道 - DEMO下载

[http://\\*\\*\\*/yzm\\_advocr/advocr.rar](http://***/yzm_advocr/advocr.rar)

支持(0) 反对(0)

### #2楼 2009-12-02 21:34 Frank Xu Lei

不错写的很详细~

支持(0) 反对(0)

### #3楼 2011-05-05 11:47 通用C#系统架构

好文档，居然在好几年前就能写好这么好的文档，佩服。

支持(0) 反对(0)

### #4楼 2016-10-03 19:48 victor0535

写得很好，很详尽，赞。有个疑问想请教一下，证书的签名部分，是对哪些信息进行的hash做的签名呢？我的猜测是 拥有者信息+public key? 怎么来验证呢 谢谢

支持(0) 反对(0)

[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】50万行VC++源码: 大型组态工控、电力仿真CAD与GIS源码库

【活动】阿里云双11活动开始预热 云服务器限时2折起

【调查】有奖调研即刻参与，你竟然是酱紫程序猿！

【推荐】Vuejs在线交互实战编程，深入浅出全面掌握



#### 最新IT新闻:

- 双十一已开战 苏宁副总裁喊话京东：手机买贵就赔
  - 妙用价格保护 京东返你1000元现金！
  - 天猫双11支付新玩法：外国人“剁手”竟如此简单
  - Instagram Stories功能日活跃用户数量达到3亿
  - 摩拜单车接入QQ扫码秒解锁，还发起了免押金和送月卡活动
- » [更多新闻...](#)



#### 最新知识库文章:

- NASA的10条代码编写原则
  - 为什么你参加了那么多培训，却依然表现平平？
  - 写给初学前端工程师的一封信
  - 实用VPC虚拟私有云设计原则
  - 如何阅读计算机科学类的书
- » [更多知识库文章...](#)

Powered by:

博客园

Copyright © chnking