



《信息安全技术》 实验报告

(Assignment 3: X.509 数字证书解
析程序设计)

学 院 名 称 : 数据科学与计算机学院

专业 (班级) : 17 软件工程 1 班

学 生 姓 名 : 陆记

学 号 : 17343080

时 间 : 2019 年 12 月 4 日

一、X.509 证书结构描述

X.509 标准定义 了被写入数字证书的信息内容，同时描述了证书内容的数据格式，证书的结构如下：

整体结构：证书内容、签名算法和签名结果，用 **ASN.1** (Abstract Syntax Notation One) 语法描述如下：

```
Certificate ::= SEQUENCE {  
    tbsCertificate      TBSCertificate, // 证书内容  
    signatureAlgorithm  AlgorithmIdentifier, // 签名算法  
    signatureValue      BIT STRING // 签名值  
}
```

1、证书内容：CA（证书颁发者）签名的信息，ASN.1 语法描述如下：

```
TBSCertificate ::= SEQUENCE {  
    version             [0] EXPLICIT Version DEFAULT v1,  
    serialNumber        CertificateSerialNumber,  
    signature            AlgorithmIdentifier,  
    issuer              Name,  
    validity            Validity,  
    subject             Name,  
    subjectPublicKeyInfo SubjectPublicKeyInfo,  
    issuerUniqueID      [1] IMPLICIT UniqueIdentifier OPTIONAL,  
    subjectUniqueID     [2] IMPLICIT UniqueIdentifier OPTIONAL,  
    extensions          [3] EXPLICIT Extensions OPTIONAL  
}
```

①**版本号 (Version)**：当前证书为哪个版本的 X.509 标准 (v1、v2、v3)，为整数格式，默认为 v1，目前最常用为 v3。其 ASN.1 语法类型 Version 的描述如下：

```
Version ::= INTEGER {v1(0), v2(1), v3(2)} // 整数0、1、2 分别表示三个版本
```

②**证书序列号 (Certificate Serial Number)**：用以区别同一实体发放的不同证书的数字序号，当某证书被吊销时，它的序列号被添加到 **CRL** 中。为整数格式，其 ASN.1 语法类型 **CertificateSerialNumber** 描述如下：

```
CertificateSerialNumber ::= INTEGER
```

③签名算法标识符 (Signature Algorithm Identifier) : 用于识别 CA 签写证书时所用的算法。其 ASN.1 语法类型 **AlgorithmIdentifier** 的描述如下: (其中, algorithm 给出算法的标识符 OID, parameters(Optional)给出了算法的参数; OID 同时说明了加密算法和数字签名算法)

```
AlgorithmIdentifier ::= SEQUENCE {
    algorithm      OBJECT IDENTIFIER, // 算法的OID
    parameters     ANY DEFINED BY algorithm OPTIONAL // 算法的参数
}
```

常用的 **OID** 如下表:

OID	Algorithm
1.2.840.10040.4.1	DSA
1.2.840.10040.4.3	sha1DSA
1.2.840.113549.1.1.1	RSA
1.2.840.113549.1.1.2	md2RSA
1.2.840.113549.1.1.3	md4RSA
1.2.840.113549.1.1.4	md5RSA
1.2.840.113549.1.1.5	sha1RSA
1.2.840.113549.1.1.11	sha256RSA

④签发人信息 (Issuer) : 签发证书的实体的 X.500 名称, 通常为 CA

⑤证书主体信息 (Subject) : 拥有证书公钥的实体的名字, 采用 X.500 标准, 在 Internet 中唯一, 是实体的特征名 (DN: Distinguished Name) 。

Issuer 和 **Subject** 的 ASN.1 语法类型都为 **Name**, 描述如下:

```
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
```

证书的 **Issuer** 和 **Subject** 用 X.509 DN 表示，DN 是由 RDN(Relative Distinguished Name)构成的序列,根据 ASN.1 语法,RDN 是由“属性类型(OID)+属性值 (STRING)” 表示，常用的属性类型名称及其 OID 如下表：

OID	属性类型名称	含义	简写
2.5.4.3	Common Name	通用名称	CN
2.5.4.6	Country	国名	C
2.5.4.7	Locality	地理位置	L
2.5.4.8	State or Province Name	洲/省名	S
2.5.4.10	Organization Name	机构名	O
2.5.4.11	Organizational Unit Name	机构单位名	OU

⑥有效期 (Validity)：包括起始时间和终止时间，每一个证书只有在该时间段内有效。有效期可以短到几秒或长至一世纪，取决于许多因素，如签写证书所用私钥的强度以及愿为证书支付的金钱等。时间值可以用 **UTCTime** 或者 **GeneralizedTime** 的形式表示。ASN.1 语法描述如下：

```
Validity ::= SEQUENCE {
    notBefore      Time,      // 起始时间
    notAfter       Time       // 截至时间
}
Time ::= CHOICE {
    utcTime        UTCTime,
    generalTime     GeneralizedTime
}
```

⑦主体公钥信息 (Subject Public Key Info)：被命名实体的公钥，包括该密钥所属公钥密码系统的算法标识符 (OID)、相关的密钥参数以及公钥值。其 ASN.1 语法描述如下：

```
SubjectPublicKeyInfo ::= SEQUENCE {
    algorithm       AlgorithmIdentifier,
    subjectPublicKey BIT STRING
}
```

⑧签发者唯一标识符和主体唯一标识符 (Issuer Unique Identifier 和 Subject Unique Identifier (Optional)) : 证书签发者和证书主体的唯一标识符。其在 ASN.1 语法中为 `UniqueIdentifier` 类型, 描述如下:

```
UniqueIdentifier ::= BIT STRING
```

⑨扩充域 (Extensions (Optional)) : 一般忽略此部分

2、证书签名算法 (Certificate Signature Algorithm) : 包括算法的标识符 (OID)、算法的参数。为 CA 对 `tbsCertificate` 进行签名所使用的算法, 类型为 `AlgorithmIdentifier` (与公钥签名算法类型一样), 其 ASN.1 语法描述如下:

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

3、签名值 (Signature Value) : 为用 X.509 标准的数字证书签名的结果, 其在 ASN.1 语法中的描述如下:

```
SignatureValue ::= BIT STRING
```

二、数据结构

1、 证书内容结构体

```
// 证书内容结构体
struct TbsCertificate {
    string version;        // 版本号
    string serialNumber;    // 序列号
    string signature[2];    // 算法OID和算法参数
    // 证书签发人和主体的属性类型 (OID) 和属性值 (STRING)
    string issuer[6][2];
    string subject[6][2];
    string validity[2];    // 有效期: 起止时间+终止时间
    string subjectPublicKeyInfo[3]; // algorithm parameters Public-key
    string issuerUniqueID;  // 签发人唯一标识符 (可选)
    string subjectUniqueID; // 主体唯一标识符 (可选)
    string extensions;     // 扩充域
};
```

2、 证书总体结构

```
// 证书总体结构
struct X509cer{
    struct TbsCertificate cer_cnt; // 证书内容
    string sig_alg[2];             // 签名算法: 算法OID+算法参数
    string sig_val;                // 签名值
};
```

3、 算法的 OID 与名称匹配表 (二维字符串数组)

```
// 签名算法OID与算法名表
string sa[8][2] = {
    {"1.2.840.10040.4.1", "DSA"},
    {"1.2.840.10040.4.3", "SHA1withDSA"},
    {"1.2.840.113549.1.1.1", "RSA"},
    {"1.2.840.113549.1.1.2", "MD2withRSA"},
    {"1.2.840.113549.1.1.3", "MD4withRSA"},
    {"1.2.840.113549.1.1.4", "MD5withRSA"},
    {"1.2.840.113549.1.1.5", "SHA1withRSA"},
    {"1.2.840.113549.1.1.11", "SHA256withRSA"}
};
```

4、 Issuer 和 Subject 信息的 OID 与其含义的匹配表 (二维字符串数组)

```
// issuer和subject名OID和对应的含义
string issu[6][2] = {
    {"2.5.4.6", "Country(C)"}, // 国名
    {"2.5.4.8", "State or Province Name(S)"}, // 洲/省名
    {"2.5.4.7", "Locality(L)"}, // 地区名
    {"2.5.4.10", "Organization Name(O)"}, // 组织名
    {"2.5.4.11", "Organizational Unit Name(OU)"}, // 组织单位名
    {"2.5.4.3", "Common Name(CN)"}, // 通用名
};
```

三、C++源代码

Github 地址:

<https://github.com/luji17343080/Information-security-technology/blob/master/X509/X509.cpp>

四、编译运行结果

控制台结果:

```
C:\Users\陆记\Desktop\大三上课程\信息安全\HW3\X509.exe
***** X.509 Certificate Resolution *****
***** By: luji17343080 *****

Version: V3
Serial Number: 2b85f2fe98d176994f38bfab9da62d5f
Algorithm of signature: SHA1withRSA
Parameters of signature: NULL
Issuer:
  Country(C): CN
  State or Province Name(S): SC
  Locality(L): CD
  Organization Name(O): UESTC
  Organizational Unit Name(OU): CS
  Common Name(CN): testCA
Validity:
  Begin: 2015.5.23 11:43:31
  End: 2020.5.23 11:52:14
Subject:
  Country(C): CN
  State or Province Name(S): SC
  Locality(L): CD
  Organization Name(O): UESTC
  Organizational Unit Name(OU): CS
  Common Name(CN): testCA
Public Key Algorithm: RSA
Public Key Parameters: 05 00
Subject Public Key:
  003082010a0282010100d49f7db04dd0136c7663ede566d0a6f7b14227326544bf96cbbc5f7a0c5762fddcae250aad8dc97cbb6a4c365
  c5c76fa856932dc92a24b63092f72db4215407a20532cc9167a58259442253dcfd38e83438e524f24965cb1fac9621069baed0858b71b178d602db9e
  9ce4a800953c17589bad04b0c8112084a5d1cb4b47d3900f7a1686e318289445408e0126c5fe973029eb35a74d8caaba57a1091f61942047bbf12d3
  e1c66e9da55558d4808dd4275aae293ad6073f20078e4566796065e6dd6157c5dd7d86693c24fa983420616731e673f0ae0bd866fc148daceb3e03b
  2aef1cc091f5b707e5d745a5f310e44c5531432ac4b99c47df54acec9d070203010001
Issuer Unique Identifier: NULL
Subject Unique Identifier: NULL
Extensions: omission
Certificate Signature Algorithm: SHA1withRSA
Parameters of Certificate Signature Algorithm: NULL
Certificate Signature:
  00689be24fac4b849bbf3763b7046561d97f79e5996f2836efd272364152489bf16131ae7f3031f751066ad84c61a3912ecec453465d279
  c12bcf97030e0205bfd78d059d6b864e6a888fc599e0f5b7336d04a3b6127a714699fc022161f348b48e3137b06c483a05e26a3ed982b513c7d73723
  38aad0052bc71c34c43ad9b3287d32c175e52790928b607f9fc489e88e32b844e50dc8918f1505c6b751ec47c0511d3512042f5272429616d2a76b3e
  62fac74213d9a8ded76302aef8ef8b74e87b226f4e2873916d57fe362f9b462c87033504ec82f6ebf8e02cdcb9a25726cd24a710c5323a77fe271387
  4532f6992aa78db08aa37d0d4b43c381a635e07ef
```

证书对比:



