X.509 Certificate

2015 级计应　　15331151　　李佳

一、X.509 证书简介

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。X.509 V4 版已经推出。它是一种行业标准或者行业解决方案，在 X.509 方案中,默认的加密体制是公钥密码体制。为进行身份认证,X.509 标准及公共密钥加密系统提供了数字签名的方案。用户可生成一段信息及其摘要(亦称作信息"指纹")。用户用专用密钥对摘要加密以形成签名,接收者用发送者的公共密钥对签名解密,并将之与收到的信息"指纹"进行比较,以确定其真实性。此问题的解决方案即 X.509 标准与公共密钥证书。本质上，证书由公共密钥加密钥拥有者的用户标识组成，整个字块有可信赖的第三方签名。典型的第三方即大型用户群体(如政府机关或金融机构)所信赖的 CA。

相关资料：　http://www.360doc.com/content/10/0401/23/633992_21238907.shtml

http://blog.csdn.net/starboybenben/article/details/48244763

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、2、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，他们分别由 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，该字段必须为非空的，除非在证书拓展中有别名

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 证书拓展部分

可选的标准和专用的拓展(仅在版本 2 和版本 3 中使用)，拓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：表示一个拓展元素的 OID

critical：表示这个拓展元素是否极重要

extnValue：表示这个拓展元素的值，字符串类型

拓展部分包括：

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 拓展标记为”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，因为该证书拓展表示相关私钥应只用于签写证书，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密钥的使用期限，它也有 Not Before 和 Not After 组成。若此项不存在时，公私钥的试用期是一样的

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 主题目录属性

指出证书拥有者的一些列属性。可以使用这一项来传递访问控制信息

X.509 文档：https://www.rfc-editor.org/rfc/rfc5280.txt

Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

三、X.509 证书实例

<1>从 RFC2459 Internet X.509 Public Key Infrastructure 标准文档中摘取的两个证书例子

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：

证书序列号是 17(0x11)

证书使用 DSA 和 SHA-1 哈希算法签名

证书发行者的名字是 OU=nist; O=gov; C=US

证书主体的名字是 OU=nist; O=gov; C=US

证书的有效期从 1997-6-30 到 1997-12-31
证书包含一个 1024 bit DSA 公钥及其参数(三个证书 p、q、g)
证书包含一个使用者密钥标识符(subjectKeyIdentifier)扩展项
证书是一个 CA 证书(通过 basicConstraints 基本扩展项标识)

地址	内容	意义
0000	30 82 02 b7	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	SEQUENCE tbsCertificate:: SEQUENCE 类型,长度 631
0008	a0 03	Version::特殊内容-证书版本(a0),长度 3
0010	02 01 02	INTEGER 2 version::整数类型(02),长度 1,版本 3(2)
0013	02 01 11	INTEGER 17 serialNumber::整数类型(02),长度 1,证书序列号 17
0016	30 09	SEQUENCE signature:: SEQUENCE 类型(30),长度 9
0018	06 07	signature:: OBJECT IDENTIFIER 类型,长度 7,dsa-with-sha 算法 OID 1.2.840.10040.4.3: dsa-with-sha
	2a 86 48 ce 38 04 03	
0027	30 2a	SEQUENCE 以下的数据块表示 issuer 信息,长度为 42
0029	31 0b	SET 开始一个集合，长度为 11
0031	30 09	SEQUENCE 开始一个序列，长度为 9
0033	06 03	OBJECT IDENTIFIER 类型,长度 3 OID 2.5.4.6 C
	55 04 06	
0038	13 02	PrintableString 'US'
	55 53	
0042	31 0c	SET 开始一个集合，长度为 12
0044	30 0a	SEQUENCE 开始一个序列，长度为 10
0046	06 03	OBJECT IDENTIFIER 类型,长度 3 OID 2.5.4.10 O
	55 04 0a	
0051	13 03	PrintableString 'gov'
	67 6f 76	
0056	31 0d	SET 开始一个集合，长度为 13
0058	30 0b	SEQUENCE 开始一个序列，长度为 11
0060	06 03	OBJECT IDENTIFIER 类型,长度 3 OID 2.5.4.11: OU
	55 04 0b	
0065	13 04	PrintableString 'nist'
	6e 69 73 74	
0071	30 1e	SEQUENCE validity:: SEQUENCE 类型(30),长度 30

0073	17 0d	notBefore:: UTCTime 类型(23),长度 13 UTCTime '9706300000000Z'
	39 37 30 36 33 30 30 30 30 30 30 30 5a	
0088	17 0d	notBefore:: UTCTime 类型(23),长度 13 UTCTime '9712310000000Z'
	39 37 31 32 33 31 30 30 30 30 30 30 5a	
0103	30 2a	SEQUENCE 以下数据块表示 subject 信息,长度 42
0105	31 0b	SET,长度 11
0107	30 09	SEQUENCE 长度 9
0109	06 03	OBJECT IDENTIFIER 类型,长度 3 OID 2.5.4.6: C
	55 04 06	
0114	13 02	PrintableString 'US'
	55 53	
0118	31 0c	SET,长度 12
0120	30 0a	SEQUENCE 长度 10
0122	06 03	OBJECT IDENTIFIER 类型,长度 3 OID 2.5.4.10: O
	55 04 0a	
0127	13 03	PrintableString 'gov'
	67 6f 76	
0132	31 0d	SET,长度 13
0134	30 0b	SEQUENCE 长度 11
0136	06 03	OBJECT IDENTIFIER 类型,长度 3 OID 2.5.4.11: OU
	55 04 0b	
0141	13 04	PrintableString 'nist'
	6e 69 73 74	
0147	30 82 01 b4	SEQUENCE subjectPublicKeyInfo::SEQUENCE 类型(30), 长度 436
0151	30 82 01 29	SEQUENCE 类型(30), 长度 297
0155	06 07	IDENTIFIER 类型,长度 7 OID 1.2.840.10040.4.1
	2a 86 48 ce 38 04 01	
0164	30 82 01 1c	SEQUENCE 类型(30), 长度 284 DSA 算法的 parameters,三个整数 p、q、g
0168	02 81 80	INTEGER p 参数，长度 128
	d4 38 02 c5 35 7b d5 0b a1 7e 5d 72 59 63 55 de 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	INTEGER q 参数，长度 20
	a7 83 9b f3 bd 2c 20 07 fc 4c e7 e8 9f f3 39 83 51 0d dc dd	
0321	02 81 80	INTEGER g 参数，长度 128
	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	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	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	extensions:: 特殊内容-证书扩展部分(a3) ，长度 50
0589	30 30	SEQUENCE, 长度 48
0591	30 0f	SEQUENCE 扩展 basicConstraints,长度 9
0593	06 03	OID 2.5.29.19: basicConstraints
	55 1d 13	
0598	01 01	BOOLEAN true，表示为 CA 证书
	ff	
0601	04 05	OCTET STRING, 长度 5

	30 03 01 01 ff	
0608	30 1d	SEQUENCE 扩展 subjectKeyIdentifier,长度 29
0610	06 03	OID 2.5.29.14: subjectKeyIdentifier
	55 1d 0e	
0615	04 16	OCTET STRING 扩展 subjectKeyIdentifier 的值，长度 22
	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	SEQUENCE signatureAlgorithm:: = AlgorithmIdentifier，长度 9
0641	06 07	OID 1.2.840.10040.4.3: dsa-with-sha
	2a 86 48 ce 38 04 03	
0650	03 2f	BIT STRING (0 unused bits) bit 串，证书签名值，47 字节
0652	30 2c	SEQUENCE，长度 44
0654	20 14	INTEGER 签名值,20 字节,160bit
	a0 66 c1 76 33 99 13 51 8d 93 64 2f cd 13 73 de 79 1a 7d 33	
0674	02 14	INTEGER 签名值,20 字节,160bit
	5d 90 f6 ce 92 4a bg 29 11 24 80 28 a6 5a 8e 73 b6 76 02 68	

<2>证书来源：http://fm4dd.com/openssl/source/DER/certs/512b-rsa-example-cert.der

内容：

```
3082 0212 3082 017b 0202 0dfa 300d 0609 2a86 4886 f70d 0101 0505 0030 819b 310b
3009 0603 5504 0613 024a 5031 0e30 0c06 0355 0408 1305 546f 6b79 6f31 1030 0e06
0355 0407 1307 4368 756f 2d6b 7531 1130 0f06 0355 040a 1308 4672 616e 6b34 4444
3118 3016 0603 5504 0b13 0f57 6562 4365 7274 2053 7570 706f 7274 3118 3016 0603
5504 0313 0f46 7261 6e6b 3444 4420 5765 6220 4341 3123 3021 0609 2a86 4886 f70d
0109 0116 1473 7570 706f 7274 4066 7261 6e6b 3464 642e 636f 6d30 1e17 0d31 3230
3832 3230 3532 3635 345a 170d 3137 3038 3231 3035 3236 3534 5a30 4a31 0b30 0906
0355 0406 1302 4a50 310e 300c 0603 5504 080c 0554 6f6b 796f 3111 300f 0603 5504
0a0c 0846 7261 6e6b 3444 4431 1830 1606 0355 0403 0c0f 7777 772e 6578 616d 706c
652e 636f 6d30 5c30 0d06 092a 8648 86f7 0d01 0101 0500 034b 0030 4802 4100 9bfc
6690 7984 42bb ab13 fd2b 7bf8 de15 12e5 f193 e306 8a7b b8b1 e19e 26bb 9501 bfe7
30ed 6485 02dd 1569 a834 b006 ec3f 353c 1e1b 2b8f fa8f 001b df07 c6ac 5307 0203
0100 0130 0d06 092a 8648 86f7 0d01 0105 0500 0381 8100 14b6 4cbb 8179 33e6 71a4
da51 6fcb 081d 8d60 ecbc 18c7 7347 59b1 f220 48bb 61fa fc4d ad89 8dd1 21eb d5d8
e5ba d6a6 36fd 7450 83b6 0fc7 1ddf 7de5 2e81 7f45 e09f e23e 79ee d730 31c7 2072
d958 2e2a fe12 5a34 45a1 1908 7c89 475f 4a95 be23 214a 5372 da2a 052f 2ec9 70f6
5bfa fddf b431 b2c1 4a9c 0625 43a1 e6b4 1e7f 869b 1640 0a
```

内容分析：

版本： V1
序列号： 0d fa
签名算法： sha1RSA
签名哈希算法： sha1
颁发者：
E = support@frank4dd.com
CN = Frank4DD Web CA
OU = WebCert Support
O = Frank4DD
L = Chuo-ku
S = Tokyo
C = JP

有效期 ： 2012.8.22 13:26:54 to 2017.8.21 13:26:54

公钥内容：

30 48 02 41 00 9b fc 66 90 79 84 42 bb ab 13 fd 2b 7b f8 de 15 12 e5 f1 93 e3 06
8a 7b b8 b1 e1 9e 26 bb 95 01 bf e7 30 ed 64 85 02 dd 15 69 a8 34 b0 06 ec 3f 35 3c 1e
1b 2b 8f fa 8f 00 1b df 07 c6 ac 53 07 02 03 01 00 01

公钥参数： 05 00

指纹算法：sha1

指纹内容：07 1c b9 4f 0c c8 51 4d 02 41 24 70 8e e8 b2 68 7b d7 d9 d5

四、工作原理

X.509 给出的鉴别框架是一种基于公开密钥体制的鉴别业务密钥管理。用户拥有两把密钥—公钥、私钥。在发送文件之前，用户可以用加密算法对信息加密，然后用接收者的公钥再次加密，而接受者就可以用自己的私钥对其解密。该框架允许用户将其公钥放在 CA 的目录项中，用户想与其他用户通信，就可以直接从对方的目录项中获得相应的公开密钥，用于各种安全服务

解析 X.509 证书过程：

1. 从磁盘上的证书文件中读取证书数据(证书数据长度)
2. 获取 CertContext
3. 获取证书信息(证书版本号、证书 SN、证书颁发者、证书主题、有效起始日期、有效终止日期)
4. 创建临时密钥容器
5. 向容器中导入公钥，获取公钥句柄
6. 导出公钥(最好采用二次调用方式)
7. 获取公钥信息
8. 清理工作