**证书解释文档**

一、环境说明

分析环境：macOS 10.14.4

测试证书：Openssl 自签名证书

测试工具：dumpasn1

二、结果说明：

证书中包含了加密方式sha256WithRSAEncryption (1 2 840 113549 1 1 11)、

注册国家countryName (2 5 4 6)、

注册城市stateOrProvinceName (2 5 4 8)、

所在区localityName (2 5 4 7)、

组织名organizationName (2 5 4 10)、

组织单位名organizationalUnitName (2 5 4 11)、

通用名commonName (2 5 4 3)、

邮箱地址emailAddress (1 2 840 113549 1 9 1)、

封装结果rsaEncryption (1 2 840 113549 1 1 1)、

主题密钥标识符authorityKeyIdentifier (2 5 29 35)

以及RSA加密结果

三、实验过程

1. dumpasn1 –h cert.der，-h参数表示将Tag和Length以十六进制形式表示出来.

<30 82 04 11>

0 1041: SEQUENCE {

<30 82 02 F9>

4 761: SEQUENCE {

<A0 03>

8 3: [0] {

<02 01>

10 1: INTEGER 2

: }

<02 09>

13 9: INTEGER 00 A0 DD 70 CE 88 E7 92 3A

<30 0D>

24 13: SEQUENCE {

<06 09>

26 9: OBJECT IDENTIFIER

: sha256WithRSAEncryption (1 2 840 113549 1 1 11)

<05 00>

37 0: NULL

: }

<30 81 9E>

39 158: SEQUENCE {

<31 0B>

42 11: SET {

<30 09>

44 9: SEQUENCE {

<06 03>

46 3: OBJECT IDENTIFIER countryName (2 5 4 6)

<13 02>

51 2: PrintableString 'CN'

: }

: }

<31 10>

55 16: SET {

<30 0E>

57 14: SEQUENCE {

<06 03>

59 3: OBJECT IDENTIFIER stateOrProvinceName (2 5 4 8)

<0C 07>

64 7: UTF8String 'Beijing'

: }

: }

<31 19>

73 25: SET {

<30 17>

75 23: SEQUENCE {

<06 03>

77 3: OBJECT IDENTIFIER localityName (2 5 4 7)

<0C 10>

82 16: UTF8String 'Haidian District'

: }

: }

<31 12>

100 18: SET {

<30 10>

102 16: SEQUENCE {

<06 03>

104 3: OBJECT IDENTIFIER organizationName (2 5 4 10)

<0C 09>

109 9: UTF8String 'BUPT SCSS'

: }

: }

<31 11>

120 17: SET {

<30 0F>

122 15: SEQUENCE {

<06 03>

124 3: OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)

<0C 08>

129 8: UTF8String '17\_CLASS'

: }

: }

<31 12>

139 18: SET {

<30 10>

141 16: SEQUENCE {

<06 03>

143 3: OBJECT IDENTIFIER commonName (2 5 4 3)

<0C 09>

148 9: UTF8String 'weehaotang'

: }

: }

<31 27>

159 39: SET {

<30 25>

161 37: SEQUENCE {

<06 09>

163 9: OBJECT IDENTIFIER emailAddress (1 2 840 113549 1 9 1)

<16 18>

174 24: IA5String 'weehaotang@outlook.com'

: }

: }

: }

<30 1E>

200 30: SEQUENCE {

<17 0D>

202 13: UTCTime 26/04/2018 10:24:28 GMT

<17 0D>

217 13: UTCTime 04/08/2018 10:24:28 GMT

: }

<30 81 9E>

232 158: SEQUENCE {

<31 0B>

235 11: SET {

<30 09>

237 9: SEQUENCE {

<06 03>

239 3: OBJECT IDENTIFIER countryName (2 5 4 6)

<13 02>

244 2: PrintableString 'CN'

: }

: }

<31 10>

248 16: SET {

<30 0E>

250 14: SEQUENCE {

<06 03>

252 3: OBJECT IDENTIFIER stateOrProvinceName (2 5 4 8)

<0C 07>

257 7: UTF8String 'Beijing'

: }

: }

<31 19>

266 25: SET {

<30 17>

268 23: SEQUENCE {

<06 03>

270 3: OBJECT IDENTIFIER localityName (2 5 4 7)

<0C 10>

275 16: UTF8String 'Haidian District'

: }

: }

<31 12>

293 18: SET {

<30 10>

295 16: SEQUENCE {

<06 03>

297 3: OBJECT IDENTIFIER organizationName (2 5 4 10)

<0C 09>

302 9: UTF8String 'BUPT SCSS'

: }

: }

<31 11>

313 17: SET {

<30 0F>

315 15: SEQUENCE {

<06 03>

317 3: OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)

<0C 08>

322 8: UTF8String '17\_CLASS'

: }

: }

<31 12>

332 18: SET {

<30 10>

334 16: SEQUENCE {

<06 03>

336 3: OBJECT IDENTIFIER commonName (2 5 4 3)

<0C 09>

341 9: UTF8String 'weehaotang'

: }

: }

<31 27>

352 39: SET {

<30 25>

354 37: SEQUENCE {

<06 09>

356 9: OBJECT IDENTIFIER emailAddress (1 2 840 113549 1 9 1)

<16 18>

367 24: IA5String 'weehaotang@outlook.com'

: }

: }

: }

<30 82 01 22>

393 290: SEQUENCE {

<30 0D>

397 13: SEQUENCE {

<06 09>

399 9: OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)

<05 00>

410 0: NULL

: }

<03 82 01 0F>

412 271: BIT STRING, encapsulates {

<30 82 01 0A>

417 266: SEQUENCE {

<02 82 01 01>

421 257: INTEGER

: 00 DA 53 F5 04 B2 10 73 F8 D7 6E 4D 5B 17 33 3E

: 12 42 69 B7 78 1F 05 E2 BE DB A8 C2 69 F7 33 B7

: 5C B3 23 29 42 AC B2 9E 90 E3 D1 E5 77 EC 6E 62

: A8 96 A9 75 75 09 BC 73 E0 42 91 74 D6 7A 52 37

: 47 F1 DC EA EF 04 66 6C 05 E0 EB 43 C9 CE CA 65

: EA BF 74 90 C1 5F 6E 06 66 0B 50 3D 08 91 D1 47

: 7B FB 59 AA 5B E4 1F 53 D2 D9 52 C8 78 20 99 3A

: 3B 59 D5 B8 AE 1A 06 67 32 B7 33 EF F0 91 CA 8A

: [ Another 129 bytes skipped ]

<02 03>

682 3: INTEGER 65537

: }

: }

: }

<A3 50>

687 80: [3] {

<30 4E>

689 78: SEQUENCE {

<30 1D>

691 29: SEQUENCE {

<06 03>

693 3: OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)

<04 16>

698 22: OCTET STRING, encapsulates {

<04 14>

700 20: OCTET STRING

: 52 DA 3A 4D 34 1B F9 AC 0A 37 47 62 C6 74 BA 67

: B8 48 EA 21

: }

: }

<30 1F>

722 31: SEQUENCE {

<06 03>

724 3: OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)

<04 18>

729 24: OCTET STRING, encapsulates {

<30 16>

731 22: SEQUENCE {

<80 14>

733 20: [0]

: 52 DA 3A 4D 34 1B F9 AC 0A 37 47 62 C6 74 BA 67

: B8 48 EA 21

: }

: }

: }

<30 0C>

755 12: SEQUENCE {

<06 03>

757 3: OBJECT IDENTIFIER basicConstraints (2 5 29 19)

<04 05>

762 5: OCTET STRING, encapsulates {

<30 03>

764 3: SEQUENCE {

<01 01>

766 1: BOOLEAN TRUE

: }

: }

: }

: }

: }

: }

<30 0D>

769 13: SEQUENCE {

<06 09>

771 9: OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)

<05 00>

782 0: NULL

: }

<03 82 01 01>

784 257: BIT STRING

: 55 DB 4E 80 2F 5A E3 8D AF 94 3B F2 D9 8F 95 66

: EF DD 4C 92 97 FA 8B 5C 54 33 75 F1 65 B7 3C F5

: CF A6 50 30 0D 79 6A D8 74 46 DB 59 A1 E4 5A 1D

: E8 6A E7 A1 86 59 3E 49 54 ED D5 8B 7E 3B D1 A0

: 87 98 B9 32 08 EB AD 89 3E A9 5A 79 23 5A 98 E7

: 79 10 2C 85 02 47 78 14 C4 C0 60 21 E0 FD CA B4

: F5 F0 44 F3 88 6D 22 69 F1 02 34 78 0D CF 79 FA

: 80 17 ED B3 58 0F 83 F1 54 C8 A5 21 3A 72 F1 58

: [ Another 128 bytes skipped ]

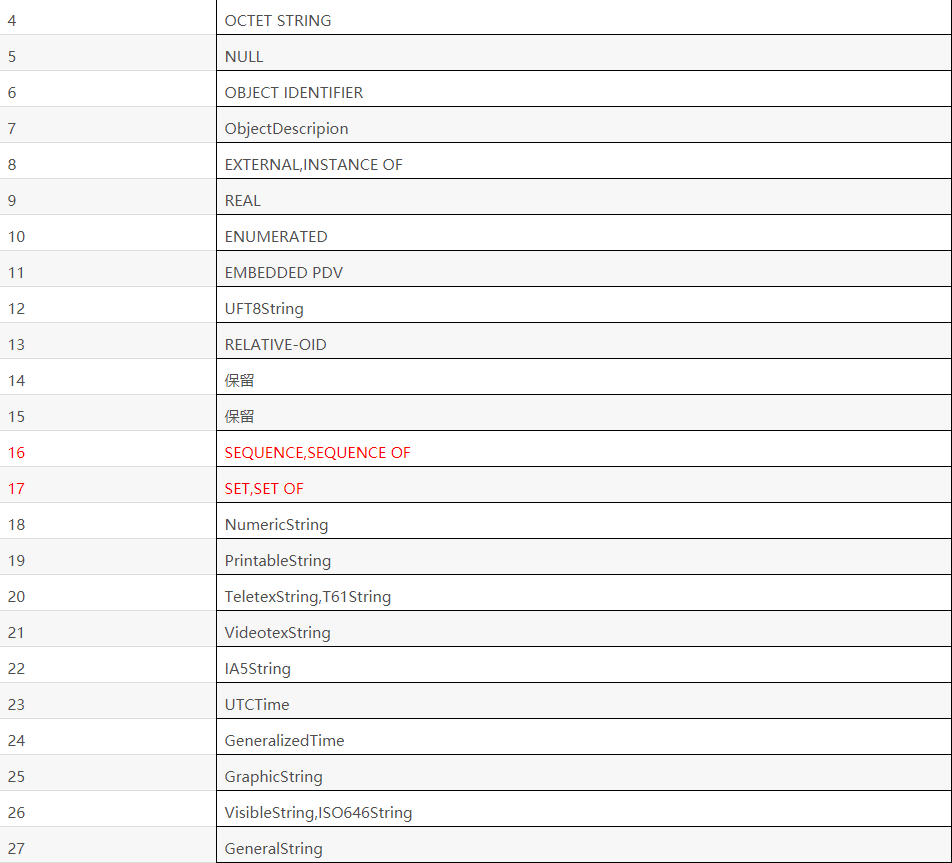
: }

2.分析

(1)这是一个嵌套的定义，最外层的SET对应的Type是31，即二进制的00110001，高二位为00，表示Universal，第六位为1，表示为构造数据类型，Tag部分为10001，为十进制的17，对应的数据类型为SET，其长度为十六进制的12，即18字节。

内部SEQUENCE对应的Type值是十六进制的30，即二进制的00110000，高二位为00表示universal，第六位为1，表示为构造数据类型，低五位Tag值是10000，即16，对应SEQUENCE，长度为0X10，即16字节。这里可以看到SET嵌套的SEQUENCE比其长度少了2字节，猜测是括号占了2字节。

SEQUENCE里包含两个成员，第一个成员的Type值是06，小于30，我们直接对应表即可查看其对应的类型是OBJECT IDENTIFIER，其长度为3字节，内容为（2 5 4 3），这个类型的对象有自己的编码规则，这里不再赘述编码。第二个成员Type值是0C，对应UTFString,长度为‘weehaotang’的字符数量：9.



（2）第二个例子是整个数据结构，由于长度过长不再截图，重点分析的是Type和Length部分，首先Type是十六进制的30，即二进制的00110000，表示通用类型，结构化数据类型，后五位10000对应SEQUENCE，长度由于大于127，不能用一个字节表示，第一个八元组的0X82即二进制10000010，第一位为1说明长度大于127，其后七位为2表示共有两个八元组来表示长度，即后面的0X0411，转换之后为十进制的1041，表示长度为1041字节，首尾花括号之间即为所有的数据内容。