X.509

jskyzero 2017/11/04

> X.509 is an ITU-T standard for a public key infrastructure (PKI) for singlesign-on (SSO, 单点登录) and Privilege Management Infrastructure (PMI,特权管理基础架构).

Give an example of X.509 certificate

We know if you want a X.509 certificate, you need a CA (Certificate Authority) process your CSR (Certificate signing request), So let's make it.

- create root CA

  1. use `ssh-keygen -f root` to produce rsa private key and SSH public key. (you can use `ssh-keygen -f root.pub -e -m pem > root.pub.pem` to format SSH public key to pem, you can alse use `ssh-keygem -f root.pub.pem -i -m pem > root2.pub` to convert back)
  2. use `openssl req -new -x509 -days 1826 -key root -out root.crt` to create root's CA, you need enter some basic information, also, you can use `openssl asn1parse -i -in root.crt` to see the details about it

```
  0:d=0  hl=4 l= 899 cons: SEQUENCE
  4:d=1  hl=4 l= 619 cons:  SEQUENCE
  8:d=2  hl=2 l=   3 cons:   cont [ 0 ]
 10:d=3  hl=2 l=   1 prim:    INTEGER           :02
 13:d=2  hl=2 l=   9 prim:   INTEGER           :E099D8E31F4D233B
 24:d=2  hl=2 l=  13 cons:   SEQUENCE
 26:d=3  hl=2 l=   9 prim:    OBJECT            :sha256WithRSAEncryption
 37:d=3  hl=2 l=   0 prim:    NULL
 39:d=2  hl=2 l=  88 cons:   SEQUENCE
 41:d=3  hl=2 l=  11 cons:    SET   43:d=4  hl=2 l=   9 cons:     SEQUENCE
 45:d=5  hl=2 l=   3 prim:      OBJECT            :countryName
 50:d=5  hl=2 l=   2 prim:      PRINTABLESTRING   :CN
 54:d=3  hl=2 l=  18 cons:    SET   56:d=4  hl=2 l=  16 cons:     SEQUENCE
 58:d=5  hl=2 l=   3 prim:      OBJECT            :stateOrProvinceName
 63:d=5  hl=2 l=   9 prim:      UTF8STRING        :GuangZHou
 74:d=3  hl=2 l=  18 cons:    SET
 76:d=4  hl=2 l=  16 cons:     SEQUENCE
 78:d=5  hl=2 l=   3 prim:      OBJECT            :localityName
 83:d=5  hl=2 l=   9 prim:      UTF8STRING        :GuangDong
 94:d=3  hl=2 l=  14 cons:    SET
 96:d=4  hl=2 l=  12 cons:     SEQUENCE
 98:d=5  hl=2 l=   3 prim:      OBJECT            :organizationName
103:d=5  hl=2 l=   5 prim:      UTF8STRING        :MOONS
110:d=3  hl=2 l=  17 cons:    SET
112:d=4  hl=2 l=  15 cons:     SEQUENCE
114:d=5  hl=2 l=   3 prim:      OBJECT            :commonName
119:d=5  hl=2 l=   8 prim:      UTF8STRING        :jskyzero
129:d=2  hl=2 l=  30 cons:   SEQUENCE
131:d=3  hl=2 l=  13 prim:    UTCTIME           :171105045005Z
146:d=3  hl=2 l=  13 prim:    UTCTIME           :221105045005Z
161:d=2  hl=2 l=  88 cons:   SEQUENCE
163:d=3  hl=2 l=  11 cons:    SET
165:d=4  hl=2 l=   9 cons:     SEQUENCE
167:d=5  hl=2 l=   3 prim:      OBJECT            :countryName
172:d=5  hl=2 l=   2 prim:      PRINTABLESTRING   :CN
176:d=3  hl=2 l=  18 cons:    SET
178:d=4  hl=2 l=  16 cons:     SEQUENCE
180:d=5  hl=2 l=   3 prim:      OBJECT            :stateOrProvinceName
185:d=5  hl=2 l=   9 prim:      UTF8STRING        :GuangZHou
196:d=3  hl=2 l=  18 cons:    SET
198:d=4  hl=2 l=  16 cons:     SEQUENCE
200:d=5  hl=2 l=   3 prim:      OBJECT            :localityName
205:d=5  hl=2 l=   9 prim:      UTF8STRING        :GuangDong
216:d=3  hl=2 l=  14 cons:    SET
218:d=4  hl=2 l=  12 cons:     SEQUENCE
220:d=5  hl=2 l=   3 prim:      OBJECT            :organizationName
225:d=5  hl=2 l=   5 prim:      UTF8STRING        :MOONS
232:d=3  hl=2 l=  17 cons:    SET
234:d=4  hl=2 l=  15 cons:     SEQUENCE
236:d=5  hl=2 l=   3 prim:      OBJECT            :commonName
241:d=5  hl=2 l=   8 prim:      UTF8STRING        :jskyzero
```

```
  251:d=2  hl=4 l= 290 cons:   SEQUENCE
  255:d=3  hl=2 l=  13 cons:    SEQUENCE
  257:d=4  hl=2 l=   9 prim:     OBJECT            :rsaEncryption
  268:d=4  hl=2 l=   0 prim:     NULL
  270:d=3  hl=4 l= 271 prim:    BIT STRING
  545:d=2  hl=2 l=  80 cons:   cont [ 3 ]
  547:d=3  hl=2 l=  78 cons:    SEQUENCE
  549:d=4  hl=2 l=  29 cons:     SEQUENCE
  551:d=5  hl=2 l=   3 prim:      OBJECT            :X509v3 Subject Key Identifier
  556:d=5  hl=2 l=  22 prim:      OCTET STRING      [HEX DUMP]:0414053370F8E9BCD35B5FF2B674559A76A216A003ED
  580:d=4  hl=2 l=  31 cons:     SEQUENCE
  582:d=5  hl=2 l=   3 prim:      OBJECT            :X509v3 Authority Key Identifier
  587:d=5  hl=2 l=  24 prim:      OCTET STRING      [HEX DUMP]:30168014053370F8E9BCD35B5FF2B674559A76A216A003ED
  613:d=4  hl=2 l=  12 cons:     SEQUENCE
  615:d=5  hl=2 l=   3 prim:      OBJECT            :X509v3 Basic Constraints
  620:d=5  hl=2 l=   5 prim:      OCTET STRING      [HEX DUMP]:30030101FF
  627:d=1  hl=2 l=  13 cons:  SEQUENCE
  629:d=2  hl=2 l=   9 prim:   OBJECT            :sha256WithRSAEncryption
  640:d=2  hl=2 l=   0 prim:   NULL
  642:d=1  hl=4 l= 257 prim:  BIT STRING
```

- create request

    1. first create user rsa private key and public key

```
# generate rsa private key
openssl genrsa 1024 > user
# (unnecessary)produce public from private key
openssl rsa -inform PEM -in user -pubout  -outform PEM -out user.pub
```

    2. create request

```
openssl req -new -key user -out user.req
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:GuangZhou
Locality Name (eg, city) []:GuangDong
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MOONS
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:jskyzero
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

# print request content
openssl asn1parse -i -in user.req
  0:d=0  hl=4 l= 408 cons: SEQUENCE
  4:d=1  hl=4 l= 257 cons:  SEQUENCE
  8:d=2  hl=2 l=   1 prim:   INTEGER           :00
 11:d=2  hl=2 l=  88 cons:   SEQUENCE
 13:d=3  hl=2 l=  11 cons:    SET
 15:d=4  hl=2 l=   9 cons:     SEQUENCE
 17:d=5  hl=2 l=   3 prim:      OBJECT            :countryName
 22:d=5  hl=2 l=   2 prim:      PRINTABLESTRING   :CN
 26:d=3  hl=2 l=  18 cons:    SET
 28:d=4  hl=2 l=  16 cons:     SEQUENCE
 30:d=5  hl=2 l=   3 prim:      OBJECT            :stateOrProvinceName
 35:d=5  hl=2 l=   9 prim:      UTF8STRING        :GuangZhou
 46:d=3  hl=2 l=  18 cons:    SET
 48:d=4  hl=2 l=  16 cons:     SEQUENCE
 50:d=5  hl=2 l=   3 prim:      OBJECT            :localityName
 55:d=5  hl=2 l=   9 prim:      UTF8STRING        :GuangDong
 66:d=3  hl=2 l=  14 cons:    SET
 68:d=4  hl=2 l=  12 cons:     SEQUENCE
 70:d=5  hl=2 l=   3 prim:      OBJECT            :organizationName
 75:d=5  hl=2 l=   5 prim:      UTF8STRING        :MOONS
 82:d=3  hl=2 l=  17 cons:    SET
 84:d=4  hl=2 l=  15 cons:     SEQUENCE
 86:d=5  hl=2 l=   3 prim:      OBJECT            :commonName
```

```
 91:d=5  hl=2 l=   8 prim:      UTF8STRING        :jskyzero
101:d=2  hl=3 l= 159 cons:   SEQUENCE
104:d=3  hl=2 l=  13 cons:    SEQUENCE
106:d=4  hl=2 l=   9 prim:     OBJECT            :rsaEncryption
117:d=4  hl=2 l=   0 prim:     NULL
119:d=3  hl=3 l= 141 prim:    BIT STRING
263:d=2  hl=2 l=   0 cons:   cont [ 0 ]
265:d=1  hl=2 l=  13 cons:  SEQUENCE
267:d=2  hl=2 l=   9 prim:   OBJECT            :sha256WithRSAEncryption
278:d=2  hl=2 l=   0 prim:   NULL
280:d=1  hl=3 l= 129 prim:  BIT STRING
```

- process request

```
openssl x509 -req -days 365 -in user.req -CA root.crt -CAkey root -set_serial 01 -out user.crt
Signature ok
subject=/C=CN/ST=GuangZhou/L=GuangDong/O=MOONS/CN=jskyzero
Getting CA Private Key
# print details
openssl asn1parse -i -in user.crt    0:d=0  hl=4 l= 672 cons: SEQUENCE
  4:d=1  hl=4 l= 392 cons:  SEQUENCE
  8:d=2  hl=2 l=   1 prim:   INTEGER           :01
 11:d=2  hl=2 l=  13 cons:   SEQUENCE
 13:d=3  hl=2 l=   9 prim:    OBJECT            :sha256WithRSAEncryption
 24:d=3  hl=2 l=   0 prim:    NULL
 26:d=2  hl=2 l=  88 cons:   SEQUENCE
 28:d=3  hl=2 l=  11 cons:    SET
 30:d=4  hl=2 l=   9 cons:     SEQUENCE
 32:d=5  hl=2 l=   3 prim:      OBJECT            :countryName
 37:d=5  hl=2 l=   2 prim:      PRINTABLESTRING   :CN
 41:d=3  hl=2 l=  18 cons:    SET
 43:d=4  hl=2 l=  16 cons:     SEQUENCE
 45:d=5  hl=2 l=   3 prim:      OBJECT            :stateOrProvinceName
 50:d=5  hl=2 l=   9 prim:      UTF8STRING        :GuangZHou
 61:d=3  hl=2 l=  18 cons:    SET
 63:d=4  hl=2 l=  16 cons:     SEQUENCE
 65:d=5  hl=2 l=   3 prim:      OBJECT            :localityName
 70:d=5  hl=2 l=   9 prim:      UTF8STRING        :GuangDong
 81:d=3  hl=2 l=  14 cons:    SET
 83:d=4  hl=2 l=  12 cons:     SEQUENCE
 85:d=5  hl=2 l=   3 prim:      OBJECT            :organizationName
 90:d=5  hl=2 l=   5 prim:      UTF8STRING        :MOONS
 97:d=3  hl=2 l=  17 cons:    SET
 99:d=4  hl=2 l=  15 cons:     SEQUENCE
101:d=5  hl=2 l=   3 prim:      OBJECT            :commonName
106:d=5  hl=2 l=   8 prim:      UTF8STRING        :jskyzero
116:d=2  hl=2 l=  30 cons:   SEQUENCE
118:d=3  hl=2 l=  13 prim:    UTCTIME           :171105051443Z
133:d=3  hl=2 l=  13 prim:    UTCTIME           :181105051443Z
148:d=2  hl=2 l=  88 cons:   SEQUENCE
150:d=3  hl=2 l=  11 cons:    SET
152:d=4  hl=2 l=   9 cons:     SEQUENCE
154:d=5  hl=2 l=   3 prim:      OBJECT            :countryName
159:d=5  hl=2 l=   2 prim:      PRINTABLESTRING   :CN
163:d=3  hl=2 l=  18 cons:    SET
165:d=4  hl=2 l=  16 cons:     SEQUENCE
167:d=5  hl=2 l=   3 prim:      OBJECT            :stateOrProvinceName
172:d=5  hl=2 l=   9 prim:      UTF8STRING        :GuangZhou
183:d=3  hl=2 l=  18 cons:    SET
185:d=4  hl=2 l=  16 cons:     SEQUENCE
187:d=5  hl=2 l=   3 prim:      OBJECT            :localityName
192:d=5  hl=2 l=   9 prim:      UTF8STRING        :GuangDong
203:d=3  hl=2 l=  14 cons:    SET
205:d=4  hl=2 l=  12 cons:     SEQUENCE
207:d=5  hl=2 l=   3 prim:      OBJECT            :organizationName
212:d=5  hl=2 l=   5 prim:      UTF8STRING        :MOONS
219:d=3  hl=2 l=  17 cons:    SET
221:d=4  hl=2 l=  15 cons:     SEQUENCE
223:d=5  hl=2 l=   3 prim:      OBJECT            :commonName
228:d=5  hl=2 l=   8 prim:      UTF8STRING        :jskyzero
238:d=2  hl=3 l= 159 cons:   SEQUENCE
241:d=3  hl=2 l=  13 cons:    SEQUENCE
243:d=4  hl=2 l=   9 prim:     OBJECT            :rsaEncryption
254:d=4  hl=2 l=   0 prim:     NULL
256:d=3  hl=3 l= 141 prim:    BIT STRING
400:d=1  hl=2 l=  13 cons:  SEQUENCE
402:d=2  hl=2 l=   9 prim:   OBJECT            :sha256WithRSAEncryption
```

```
    413:d=2  hl=2 l=   0 prim:   NULL
    415:d=1  hl=4 l= 257 prim:  BIT STRING
```

以上，虽然没有自己编程查看具体的数据字段内容，但是完整了模拟了整个证书申请的过程，并查看了证书的主要字段的内容，至于具体字段的分布，可以参考下面的RFC文档。

How it works

X509主要解决的问题是公钥发布，我们将证书交给去权威机构发布，权威机构的公钥是大家都知道的，因而可以安全和它通信，权威机构的每份证书包含一些关键字段（比如机构/路径/有效时间等），还需要拥有者的私钥的签名，这样就可以安全的将公钥发布。

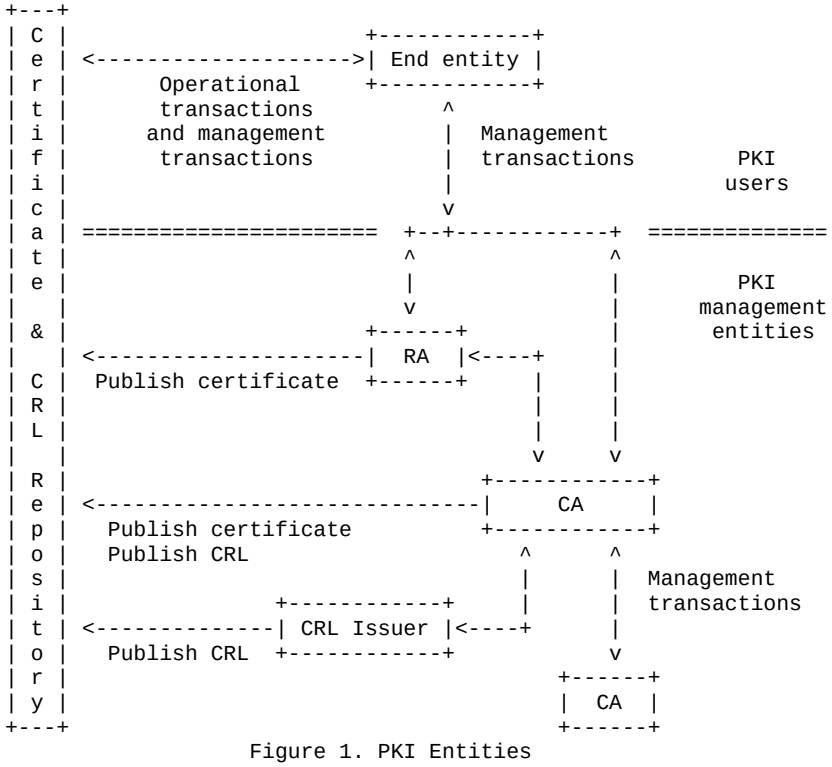

Figure 1. PKI Entities

Reference

- rfc5280
- certexamples-creation
- howto-make-your-own-cert-with-openssl