Certificates with OpenSSL

Giuseppe Persiano

Università di Salerno

November, 2020

Two-Level CA

Two-Level CA

- One *Root CA* that produces certificats for the *Intermediate CA*
- One or more *Intermediate CA*s that produce certificates for *clients* and *servers*

Setting up the folder for a CA

The CA needs the following directories:

- `certs`: to store own certificate
- `private`: to store own private key
- `newcerts`: to store signed certificates indexed by serial number
- `crl`: to store the certificate revocation lists
- `csr`: to store the certificate signing requests

and the following files

- `serial`: holds the serial number of the next certificate
- `index.txt`: DNs of the signed certificates

Setting up the Root Certificate

Root CA

A two-step process:

- Generate the private key
  `openssl genrsa -aes256 -out private/cakey.pem 4096`
  Protect the private key by making it readable only to owner
- Produce the certificate by signing the public key
  Self-sign the public key with the command
  `openssl req -new`
  - `-x509` self signed
  - `-config` the configuration file to be used
  - `-extensions` the section of the configuration file

  Protect the certificate by making it only readable

See script `createRootCert.sh`

What is in the Root CA

```
    Data:
        Version: 3 (0x2)
        Serial Number:
            3d:60:76:e7:75:ab:4b:ed:e2:d7:37:6e:17:07:53:18:05:66:34:30
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = IT, ST = Campania, L = Salerno, O = UNISA -- Corso Persiano
 CN = RootCA, emailAddress = pino.persiano@unisa.it
        Validity
            Not Before: Nov 22 21:29:32 2020 GMT
            Not After : Nov 17 21:29:32 2040 GMT
        Subject: C = IT, ST = Campania, L = Salerno, O = UNISA -- Corso Persian
, CN = RootCA, emailAddress = pino.persiano@unisa.it
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:d4:99:80:ed:af:40:fa:71:45:b2:30:11:3e:c4:
                    ec:b4:dd:c9:b5:44:93:6c:41:df:3b:45:43:6e:7a:
                    aa:89:a5:2d:23:d3:7b:5c:18:23:cd:55:65:5f:22:
                    93:9a:b8:bd:ac:a1:95:59:ef:00:81:02:45:6a:01:
                    d0:d7:34:94:52:60:7d:59:79:3c:3f:ad:ee:1c:63:
                    0d:fd:b1:d1:1f:56:f0:1a:0f:92:36:1f:fb:c4:4a:
                    59:14:f5:23:cb:d1:d0:dd:8c:bf:ea:0c:f0:84:a6:
```

Setting up the Intermediate Certificate

Intermediate CA: a three-step process

- Generate the private key [`createIntermediate.sh`]
  `openssl genrsa -aes256 -out private/cakey.pem 4096`
  Protect the private key by making it readable only to owner
- Generate a Certificate Signing Request for the Root CA
  [`createIntermediate.sh`]
  `openssl req`
  - `-config` specifies the configuration file to be used
  - `-key` specifies the key to be certified
  - `-out` file containing the CSR output
- Sign the CSR using the Root CA private key
  [`signIntermediate.sh`]
  `openssl ca`
  - `-config` configuration file
  - `-extensions` section of the configuration file

  Create the chain of certificates:
  concatenate the new certificate and the root's self-signed certificate

Verifying the intermediate certificate

```
openssl verify -CAfile RootCert IntermediateCert
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = IT, ST = Campania, L = Salerno, O = UNISA -- Corso Persiano,
 CN = RootCA, emailAddress = pino.persiano@unisa.it
        Validity
            Not Before: Nov 22 21:57:28 2020 GMT
            Not After : Nov 20 21:57:28 2030 GMT
        Subject: C = IT, ST = Campania, O = UNISA -- Corso Persiano, CN = Interm
ediate CA, emailAddress = pino.persiano@unisa.it
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:e0:f0:04:6b:1a:a7:17:ba:86:6e:cd:d2:cb:9f:
                    d8:ce:02:b7:ea:9c:8d:22:7a:ad:25:ee:90:46:a9:
                    6f:12:f8:06:08:78:74:9e:ad:1e:28:1e:3a:c8:f0:
```

Producing certificates

Client certificate: a three-step process

- Generate the private key [`createClient.sh`]
  `openssl genrsa -aes256 -out aa@aa.com.key.pem 4096`
- Generate a Certificate Signing Request for the Intermediate CA [`createClient.sh`]
  `openssl req`
  - `-config` specifies the configuration file to be used
  - `-key` specifies the key to be certified
  - `-out` file containing the CSR output
- Sign the CSR using the Intermediate CA private key [`createClient.sh`]
  `openssl ca`
  - `-config` configuration file
  - `-extensions` section of the configuration file
    use the user section or the server section

Inspecting the client certificate

```
openssl x509 -noout -text -in certs/aa@aa.com.cert.pem
```

```
    Data:
        Version: 3 (0x2)
        Serial Number: 4098 (0x1002)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = IT, ST = Campania, O = UNISA -- Corso Persiano, CN = Interme
diate CA, emailAddress = pino.persiano@unisa.it
        Validity
            Not Before: Nov 22 22:30:40 2020 GMT
            Not After : Dec  2 22:30:40 2021 GMT
        Subject: C = IT, ST = Campania, L = Salerno, O = UNISA -- Corso Persiano
, CN = AA, emailAddress = aa@aa.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:de:0a:6a:9d:4f:4a:42:cc:32:4d:a7:0b:c3:30:
                    fb:62:75:24:f3:ef:86:58:14:d5:bc:31:16:05:5a:
                    a7:c3:73:5a:fe:9d:32:96:0d:e7:f2:d7:59:da:74:
                    5a:b3:da:07:cd:79:1d:46:0f:fa:12:e4:c2:ad:16:
                    fe:55:fb:21:a8:35:c1:d1:71:9f:42:8b:97:5e:b5:
                    56:25:82:b1:16:db:e2:ab:70:6c:90:a8:0c:ae:92:
                    9e:5f:5b:dd:02:66:51:d5:a0:71:3c:4d:2e:7d:57:
```

Inspecting the client certificate

```
openssl x509 -noout -text -in certs/aa@aa.com.cert.pem
```

```
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Client, S/MIME
            Netscape Comment:
                OpenSSL Generated Client Certificate
            X509v3 Subject Key Identifier:
                D3:1F:17:9A:C9:C2:D0:0F:74:CA:16:DB:D7:2C:64:5E:E1:B7:4B:8C
            X509v3 Authority Key Identifier:
                keyid:39:19:08:F3:E4:C6:A2:C7:2A:97:B8:62:62:01:66:21:10:15:39:
3

            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection
    Signature Algorithm: sha256WithRSAEncryption
```

Inspecting the server certificate

```
openssl x509 -noout -text -in certs/www.example.com.cert.pem
```

```
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = IT, ST = Campania, O = UNISA -- Corso Persiano, CN = Inter
diate CA, emailAddress = pino.persiano@unisa.it
        Validity
            Not Before: Nov 22 22:08:21 2020 GMT
            Not After : Dec  2 22:08:21 2021 GMT
        Subject: C = IT, ST = Campania, L = Salerno, O = UNISA -- Corso Persia
, CN = www.example.com, emailAddress = pino.persiano@unisa.it
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:96:eb:98:81:3b:ad:bf:8f:b3:8e:7d:5b:6d:89:
                    b6:5b:2a:56:95:5d:a9:05:29:37:9b:80:a3:ae:fa:
                    02:33:52:72:17:ee:5f:2c:36:de:4b:15:09:e4:77:
                    97:0d:d8:d0:2c:12:d4:83:68:ac:e5:fc:48:49:3e:
                    13:6c:00:de:fc:47:22:f0:52:c7:9e:5c:c2:d1:e9:
```

Inspecting the server certificate

`openssl x509 -noout -text -in certs/www.example.com.cert.pem`

```
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Server
            Netscape Comment:
                OpenSSL Generated Server Certificate
            X509v3 Subject Key Identifier:
                4B:59:17:8C:7A:05:B7:6F:F5:CE:2A:5C:66:9B:5B:62:BF:37:A4:0B
            X509v3 Authority Key Identifier:
                keyid:39:19:08:F3:E4:C6:A2:C7:2A:97:B8:62:62:01:66:21:10:15:39:9
3
                DirName:/C=IT/ST=Campania/L=Salerno/O=UNISA -- Corso Persiano/CN
=RootCA/emailAddress=pino.persiano@unisa.it
                serial:10:00

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
    Signature Algorithm: sha256WithRSAEncryption
```