```
Last login: Thu Nov 26 19:55:33 on ttys001
haduong@Has-MacBook-Air ~ % cd Desktop
haduong@Has-MacBook-Air Desktop % cd PKI
haduong@Has-MacBook-Air PKI % git clone https://bitbucket.org/stefanholek/pki-ex
ample-1
Cloning into 'pki-example-1'...
remote: Counting objects: 48, done.
remote: Compressing objects: 100% (37/37), done.
remote: Total 48 (delta 20), reused 0 (delta 0)
Unpacking objects: 100% (48/48), done.
haduong@Has-MacBook-Air PKI % cd pki-example-1
haduong@Has-MacBook-Air pki-example-1 % mkdir -p ca/root-ca/private ca/root-ca/d
b crl certs
haduong@Has-MacBook-Air pki-example-1 % chmod 700 ca/root-ca/private
haduong@Has-MacBook-Air pki-example-1 % cp /dev/null ca/root-ca/db/root-ca.db
haduong@Has-MacBook-Air pki-example-1 % cp /dev/null ca/root-ca/db/root-ca.db.at
tr
haduong@Has-MacBook-Air pki-example-1 % echo 01 > ca/root-ca/db/root-ca.crt.srl
haduong@Has-MacBook-Air pki-example-1 % echo 01 > ca/root-ca/db/root-ca.crl.srl
haduong@Has-MacBook-Air pki-example-1 % openssl req -new \
    -config etc/root-ca.conf \
    -out ca/root-ca.csr \
    -keyout ca/root-ca/private/root-ca.key
Generating a 2048 bit RSA private key
.........................................+++
.................................+++
writing new private key to 'ca/root-ca/private/root-ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
haduong@Has-MacBook-Air pki-example-1 % openssl ca -selfsign \
    -config etc/root-ca.conf \
    -in ca/root-ca.csr \
    -out ca/root-ca.crt \
    -extensions root_ca_ext
Using configuration from etc/root-ca.conf
Enter pass phrase for ./ca/root-ca/private/root-ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Nov 27 05:03:27 2020 GMT
            Not After : Nov 27 05:03:27 2030 GMT
        Subject:
            domainComponent           = org
            domainComponent           = simple
            organizationName          = Simple Inc
            organizationalUnitName    = Simple Root CA
            commonName                = Simple Root CA
        X509v3 extensions:
            X509v3 Key Usage: critical
```

```
                Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                31:5E:EC:D0:41:B3:76:6D:6C:08:C5:95:49:42:B0:D2:9F:1D:E6:27
            X509v3 Authority Key Identifier:
                keyid:31:5E:EC:D0:41:B3:76:6D:6C:08:C5:95:49:42:B0:D2:9F:1D:E6:2
7

Certificate is to be certified until Nov 27 05:03:27 2030 GMT (3652 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
haduong@Has-MacBook-Air pki-example-1 % mkdir -p ca/signing-ca/private ca/signin
g-ca/db crl certs
haduong@Has-MacBook-Air pki-example-1 % chmod 700 ca/signing-ca/private
haduong@Has-MacBook-Air pki-example-1 % cp /dev/null ca/signing-ca/db/signing-ca
.db
haduong@Has-MacBook-Air pki-example-1 % cp /dev/null ca/signing-ca/db/signing-ca
.db.attr
haduong@Has-MacBook-Air pki-example-1 % echo 01 > ca/signing-ca/db/signing-ca.cr
t.srl
haduong@Has-MacBook-Air pki-example-1 % echo 01 > ca/signing-ca/db/signing-ca.cr
l.srl
haduong@Has-MacBook-Air pki-example-1 % openssl req -new \
    -config etc/signing-ca.conf \
    -out ca/signing-ca.csr \
    -keyout ca/signing-ca/private/signing-ca.key
Generating a 2048 bit RSA private key
..............+++
..............................+++
writing new private key to 'ca/signing-ca/private/signing-ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
haduong@Has-MacBook-Air pki-example-1 % openssl ca \
    -config etc/root-ca.conf \
    -in ca/signing-ca.csr \
    -out ca/signing-ca.crt \
    -extensions signing_ca_ext
Using configuration from etc/root-ca.conf
Enter pass phrase for ./ca/root-ca/private/root-ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 2 (0x2)
        Validity
            Not Before: Nov 27 05:05:32 2020 GMT
            Not After : Nov 27 05:05:32 2030 GMT
```

```
        Subject:
            domainComponent           = org
            domainComponent           = simple
            organizationName          = Simple Inc
            organizationalUnitName    = Simple Signing CA
            commonName                = Simple Signing CA
        X509v3 extensions:
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Subject Key Identifier:
                3A:46:CC:8E:7B:00:F1:A8:8A:54:CF:D0:BC:1A:A2:4D:F4:0E:C3:BB
            X509v3 Authority Key Identifier:
                keyid:31:5E:EC:D0:41:B3:76:6D:6C:08:C5:95:49:42:B0:D2:9F:1D:E6:2
7

Certificate is to be certified until Nov 27 05:05:32 2030 GMT (3652 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
haduong@Has-MacBook-Air pki-example-1 % openssl req -new \
    -config etc/email.conf \
    -out certs/fred.csr \
    -keyout certs/fred.key
Generating a 2048 bit RSA private key
.....................................................+++
...+++
writing new private key to 'certs/fred.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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.
-----
1. Domain Component         (eg, com)       []:org
2. Domain Component         (eg, company)   []:simple
3. Domain Component         (eg, pki)       []:.
4. Organization Name        (eg, company)   []:Simple Inc
5. Organizational Unit Name (eg, section)   []:.
6. Common Name              (eg, full name) []:Fred Flintstone
7. Email Address            (eg, name@fqdn) []:fred@simple.org
haduong@Has-MacBook-Air pki-example-1 % openssl ca \
    -config etc/signing-ca.conf \
    -in certs/fred.csr \
```

```
    -out certs/fred.crt \
    -extensions email_ext
Using configuration from etc/signing-ca.conf
Enter pass phrase for ./ca/signing-ca/private/signing-ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Nov 27 05:07:27 2020 GMT
            Not After : Nov 27 05:07:27 2022 GMT
        Subject:
            domainComponent           = org
            domainComponent           = simple
            organizationName          = Simple Inc
            commonName                = Fred Flintstone
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                E-mail Protection, TLS Web Client Authentication
            X509v3 Subject Key Identifier:
                C0:67:48:16:86:B3:73:C2:5F:6F:30:F8:FA:2B:1C:59:B6:47:2E:5D
            X509v3 Authority Key Identifier:
                keyid:3A:46:CC:8E:7B:00:F1:A8:8A:54:CF:D0:BC:1A:A2:4D:F4:0E:C3:B
B

            X509v3 Subject Alternative Name:
                email:fred@simple.org
Certificate is to be certified until Nov 27 05:07:27 2022 GMT (730 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
haduong@Has-MacBook-Air pki-example-1 % SAN=DNS:www.simple.org \
openssl req -new \
    -config etc/server.conf \
    -out certs/simple.org.csr \
    -keyout certs/simple.org.key
Generating a 2048 bit RSA private key
.+++
.....................+++
writing new private key to 'certs/simple.org.key'
-----
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.
-----
1. Domain Component         (eg, com)       []:org
2. Domain Component         (eg, company)   []:simple
3. Domain Component         (eg, pki)       []:.
4. Organization Name        (eg, company)   []:Simple Inc
5. Organizational Unit Name (eg, section)   []:.
6. Common Name              (eg, FQDN)      []:www.simple.org
haduong@Has-MacBook-Air pki-example-1 % openssl ca \
    -config etc/signing-ca.conf \
    -in certs/simple.org.csr \
    -out certs/simple.org.crt \
    -extensions server_ext
Using configuration from etc/signing-ca.conf
Enter pass phrase for ./ca/signing-ca/private/signing-ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 2 (0x2)
        Validity
            Not Before: Nov 27 05:08:49 2020 GMT
            Not After : Nov 27 05:08:49 2022 GMT
        Subject:
            domainComponent           = org
            domainComponent           = simple
            organizationName          = Simple Inc
            commonName                = www.simple.org
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Subject Key Identifier:
                CA:D3:8E:3E:B5:FD:45:B2:4D:E1:0C:20:5E:E2:0A:D1:05:FD:5A:98
            X509v3 Authority Key Identifier:
                keyid:3A:46:CC:8E:7B:00:F1:A8:8A:54:CF:D0:BC:1A:A2:4D:F4:0E:C3:B
B

            X509v3 Subject Alternative Name:
                DNS:yourdomain.tld
Certificate is to be certified until Nov 27 05:08:49 2022 GMT (730 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
haduong@Has-MacBook-Air pki-example-1 % openssl ca \
    -config etc/signing-ca.conf \
```

```
    -revoke ca/signing-ca/01.pem \
    -crl_reason superseded
Using configuration from etc/signing-ca.conf
Enter pass phrase for ./ca/signing-ca/private/signing-ca.key:
Revoking Certificate 01.
Data Base Updated
haduong@Has-MacBook-Air pki-example-1 % openssl ca -gencrl \
    -config etc/signing-ca.conf \
    -out crl/signing-ca.crl
Using configuration from etc/signing-ca.conf
Enter pass phrase for ./ca/signing-ca/private/signing-ca.key:
haduong@Has-MacBook-Air pki-example-1 % openssl x509 \
    -in certs/fred.crt \
    -out certs/fred.cer \
    -outform der
haduong@Has-MacBook-Air pki-example-1 % openssl crl \
    -in crl/signing-ca.crl \
    -out crl/signing-ca.crl \
    -outform der
haduong@Has-MacBook-Air pki-example-1 % openssl crl2pkcs7 -nocrl \
    -certfile ca/signing-ca.crt \
    -certfile ca/root-ca.crt \
    -out ca/signing-ca-chain.p7c \
    -outform der
haduong@Has-MacBook-Air pki-example-1 % openssl pkcs12 -export \
    -name "Fred Flintstone" \
    -inkey certs/fred.key \
    -in certs/fred.crt \
    -out certs/fred.p12
Enter pass phrase for certs/fred.key:
Enter Export Password:
Verifying - Enter Export Password:
haduong@Has-MacBook-Air pki-example-1 % cat ca/signing-ca.crt ca/root-ca.crt > \

    ca/signing-ca-chain.pem
haduong@Has-MacBook-Air pki-example-1 % cat certs/fred.key certs/fred.crt > \
    certs/fred.pem
haduong@Has-MacBook-Air pki-example-1 % openssl req \
    -in certs/fred.csr \
    -noout \
    -text
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: DC=org, DC=simple, O=Simple Inc, CN=Fred Flintstone
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b8:bb:66:2e:fa:23:81:2f:bf:5f:35:91:70:9f:
                    ac:9d:94:fd:21:4e:66:24:7b:b1:75:c5:5d:c4:26:
                    05:af:7b:b6:c2:6e:8e:42:5f:7a:49:60:8b:55:39:
```

```
                    e0:7b:2f:3e:61:27:5f:5e:0c:ef:5e:f1:15:c7:4c:
                    e2:21:f6:80:8c:ff:2e:69:3e:e0:0e:7b:1a:63:2d:
                    68:66:2e:87:17:ff:60:3d:d5:12:47:4a:41:db:55:
                    0f:a7:e1:cf:1c:32:5b:c8:af:ca:7d:04:11:01:fa:
                    ea:7a:7c:a4:3d:ac:90:c0:d3:86:27:78:1f:3f:85:
                    af:e4:00:f7:e0:6d:f9:e0:eb:72:03:d3:7b:0e:cc:
                    10:98:13:85:f1:bd:85:9e:66:d4:4f:3c:99:cb:69:
                    c5:27:04:90:97:5c:17:f6:af:26:93:87:ff:80:8c:
                    f1:dd:a7:6e:50:35:e6:f1:dc:46:2f:b6:be:1b:9d:
                    14:a7:3c:45:4a:50:e7:f1:4e:81:9c:86:b2:5b:7e:
                    eb:98:76:f0:15:c9:e6:25:0e:4b:8b:f7:53:07:da:
                    c4:de:f6:48:b4:14:fe:f1:4e:58:a2:55:de:24:35:
                    f0:3d:1b:5a:6e:70:c2:c0:8d:0d:11:17:8e:29:f0:
                    71:c1:a8:51:40:83:0e:41:a1:fe:58:96:2e:71:a4:
                    8d:91
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                E-mail Protection, TLS Web Client Authentication
            X509v3 Subject Key Identifier:
                C0:67:48:16:86:B3:73:C2:5F:6F:30:F8:FA:2B:1C:59:B6:47:2E:5D
            X509v3 Subject Alternative Name:
                email:fred@simple.org
    Signature Algorithm: sha1WithRSAEncryption
         5e:a5:d2:88:39:d2:4b:d4:aa:ec:59:be:9d:81:26:2d:47:88:
         41:89:23:a4:31:82:33:5c:5d:8c:e8:f6:fd:14:11:10:f7:55:
         f6:27:8a:f7:ff:1e:32:a8:84:c3:b5:06:94:1c:fa:51:17:1b:
         65:28:30:cf:cb:86:e8:9d:53:1c:44:98:c0:c7:3a:ae:b6:71:
         28:4c:4f:11:48:c6:70:93:96:fa:3b:fa:6f:5c:5c:9c:2e:6c:
         fe:01:04:da:69:7b:72:6f:06:ed:df:1a:d8:13:90:f5:89:55:
         22:4a:89:83:45:91:da:23:46:fa:b3:42:73:ee:5c:27:dc:19:
         6e:c7:11:56:a9:a8:86:46:ab:d7:af:a9:98:50:1a:e7:a9:da:
         0f:81:d1:a3:37:eb:dd:69:9c:a6:af:e3:3a:ca:ad:97:c5:c0:
         1e:63:20:ff:5e:0b:2e:f2:44:b3:bf:71:dd:09:b6:5d:c7:4b:
         1c:a4:d4:50:58:14:a2:78:bb:95:3b:56:67:f1:f3:fa:60:f5:
         11:5a:be:89:c0:fb:07:6f:33:1b:bc:62:85:75:f0:86:54:21:
         b7:1b:91:39:54:39:ab:c3:5e:b7:fe:d3:74:c3:f1:c0:bb:d0:
         2a:44:8e:6c:77:1d:56:00:2b:3a:7b:17:be:6f:57:b6:0b:20:
         f6:a8:8e:d6
haduong@Has-MacBook-Air pki-example-1 % openssl x509 \
    -in certs/fred.crt \
    -noout \
    -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: DC=org, DC=simple, O=Simple Inc, OU=Simple Signing CA, CN=Simple
```

```
 Signing CA
        Validity
            Not Before: Nov 27 05:07:27 2020 GMT
            Not After : Nov 27 05:07:27 2022 GMT
        Subject: DC=org, DC=simple, O=Simple Inc, CN=Fred Flintstone
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b8:bb:66:2e:fa:23:81:2f:bf:5f:35:91:70:9f:
                    ac:9d:94:fd:21:4e:66:24:7b:b1:75:c5:5d:c4:26:
                    05:af:7b:b6:c2:6e:8e:42:5f:7a:49:60:8b:55:39:
                    e0:7b:2f:3e:61:27:5f:5e:0c:ef:5e:f1:15:c7:4c:
                    e2:21:f6:80:8c:ff:2e:69:3e:e0:0e:7b:1a:63:2d:
                    68:66:2e:87:17:ff:60:3d:d5:12:47:4a:41:db:55:
                    0f:a7:e1:cf:1c:32:5b:c8:af:ca:7d:04:11:01:fa:
                    ea:7a:7c:a4:3d:ac:90:c0:d3:86:27:78:1f:3f:85:
                    af:e4:00:f7:e0:6d:f9:e0:eb:72:03:d3:7b:0e:cc:
                    10:98:13:85:f1:bd:85:9e:66:d4:4f:3c:99:cb:69:
                    c5:27:04:90:97:5c:17:f6:af:26:93:87:ff:80:8c:
                    f1:dd:a7:6e:50:35:e6:f1:dc:46:2f:b6:be:1b:9d:
                    14:a7:3c:45:4a:50:e7:f1:4e:81:9c:86:b2:5b:7e:
                    eb:98:76:f0:15:c9:e6:25:0e:4b:8b:f7:53:07:da:
                    c4:de:f6:48:b4:14:fe:f1:4e:58:a2:55:de:24:35:
                    f0:3d:1b:5a:6e:70:c2:c0:8d:0d:11:17:8e:29:f0:
                    71:c1:a8:51:40:83:0e:41:a1:fe:58:96:2e:71:a4:
                    8d:91
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                E-mail Protection, TLS Web Client Authentication
            X509v3 Subject Key Identifier:
                C0:67:48:16:86:B3:73:C2:5F:6F:30:F8:FA:2B:1C:59:B6:47:2E:5D
            X509v3 Authority Key Identifier:
                keyid:3A:46:CC:8E:7B:00:F1:A8:8A:54:CF:D0:BC:1A:A2:4D:F4:0E:C3:B
B

            X509v3 Subject Alternative Name:
                email:fred@simple.org
    Signature Algorithm: sha1WithRSAEncryption
         b4:0b:71:e9:27:2c:17:41:31:46:b2:ab:65:0c:53:e4:ae:01:
         9f:b0:e4:9d:38:17:7f:ce:f2:63:b0:c7:87:f3:76:22:04:7e:
         ac:85:2b:bd:67:93:4f:ba:49:64:d6:68:83:e1:2d:54:fd:54:
         c4:70:c8:b0:1c:3e:3e:c4:33:50:c6:40:19:70:45:05:79:8d:
         82:81:9b:2f:c1:8c:ad:97:aa:e4:48:59:e1:56:d1:d6:5b:37:
         97:2f:55:c1:4f:f6:bc:87:3b:ce:2a:6a:95:68:b4:ab:5e:49:
         62:e2:b2:32:d9:53:a7:81:b6:53:a4:b3:24:b5:da:e5:df:7a:
         f3:97:43:d4:3a:a0:31:67:ec:ca:f7:2c:42:34:fd:07:74:03:
```

```
         d5:e8:e8:d2:6c:52:92:44:6c:76:24:a1:5b:fb:56:71:6a:70:
         b6:26:d5:1b:45:b3:1e:38:72:cc:44:1e:94:e5:73:7b:c7:84:
         af:60:0b:00:16:49:e6:3a:aa:0d:ce:39:3d:ec:0a:0c:55:c7:
         a4:43:59:44:5a:27:c1:9c:f6:98:72:b2:29:61:a1:30:52:21:
         b8:32:9a:bf:e8:c8:e5:38:1c:38:9a:7c:d1:88:ee:98:2a:d3:
         e7:b1:b2:4e:d1:04:2e:c1:6d:94:e6:16:96:36:82:c5:14:7e:
         33:fc:a4:b0
haduong@Has-MacBook-Air pki-example-1 % openssl crl \
    -in crl/signing-ca.crl \
    -inform der \
    -noout \
    -text
Certificate Revocation List (CRL):
        Version 2 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: /DC=org/DC=simple/O=Simple Inc/OU=Simple Signing CA/CN=Simple Si
gning CA
        Last Update: Nov 27 05:09:47 2020 GMT
        Next Update: Dec  4 05:09:47 2020 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
                keyid:3A:46:CC:8E:7B:00:F1:A8:8A:54:CF:D0:BC:1A:A2:4D:F4:0E:C3:B
B

            X509v3 CRL Number:
                1
Revoked Certificates:
    Serial Number: 01
        Revocation Date: Nov 27 05:09:17 2020 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Superseded
    Signature Algorithm: sha1WithRSAEncryption
         6d:ae:b3:a4:26:a9:d7:01:ba:b2:67:40:9c:d1:cf:14:4d:62:
         8b:52:a9:55:ee:1b:3f:09:49:49:fc:dc:3d:47:7f:43:fa:20:
         19:52:96:2a:e1:1f:59:c9:88:7a:b5:a2:8c:44:42:0b:8b:d0:
         10:cb:66:54:a0:cb:09:20:9f:19:d7:7a:bb:6d:53:30:89:56:
         4c:8b:ab:17:59:83:b6:3b:5d:2c:9f:03:63:1a:83:70:d5:2e:
         10:3b:87:6a:3d:f5:2a:6a:ef:1e:91:a5:e4:99:3d:16:05:a3:
         e7:30:00:7d:25:7a:ba:34:b6:0d:1c:35:fb:45:20:37:83:dd:
         98:cb:37:4d:a5:c1:9f:2c:db:4c:66:38:1d:37:22:05:fd:f6:
         19:f9:28:57:ba:f7:5e:66:8c:9c:b6:fa:8f:ce:aa:10:06:f5:
         98:b5:39:fd:51:e1:93:87:3b:55:f1:ee:60:60:5c:9a:3b:42:
         87:7c:5a:df:98:ad:72:ec:46:d1:be:da:83:88:4d:d5:d4:e8:
         11:fa:f9:53:d8:c4:6b:c0:31:0c:b8:8c:30:0a:10:5a:77:fc:
         c0:1e:5d:63:76:84:a9:7a:e3:1b:5e:fe:eb:e4:7d:e6:86:e3:
         fc:4d:04:89:94:3d:3f:12:3f:03:0a:bd:85:46:22:dc:f3:e5:
         b6:11:4c:e0
haduong@Has-MacBook-Air pki-example-1 % openssl pkcs7 \
    -in ca/signing-ca-chain.p7c \
    -inform der \
    -noout \
```

```
    -text \
    -print_certs
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: DC=org, DC=simple, O=Simple Inc, OU=Simple Root CA, CN=Simple Ro
ot CA
        Validity
            Not Before: Nov 27 05:05:32 2020 GMT
            Not After : Nov 27 05:05:32 2030 GMT
        Subject: DC=org, DC=simple, O=Simple Inc, OU=Simple Signing CA, CN=Simpl
e Signing CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:dd:82:88:27:f0:ff:0e:a4:63:1d:ca:f8:da:12:
                    d1:b4:28:c5:4b:06:91:75:2f:58:15:71:e0:e4:a2:
                    b3:d8:74:d2:6e:3f:bb:40:a7:72:19:0c:cc:b0:2e:
                    85:cc:6e:60:2b:fc:80:61:9a:94:f2:03:0a:0a:81:
                    73:0c:11:8b:4e:4d:ea:30:85:e6:fd:e7:be:11:e7:
                    b4:04:fd:66:f0:bf:ec:43:14:c0:ac:a1:6e:8b:f2:
                    f3:ff:d3:7d:71:a2:b2:c1:bb:3c:16:49:f6:f5:fb:
                    d9:1c:3a:05:5b:49:cd:74:e2:f7:99:34:69:a8:a2:
                    e4:66:37:42:e9:b3:bf:36:7a:84:a8:8b:35:d6:ad:
                    fe:fc:b5:04:29:db:9f:f6:d7:03:9f:db:e2:25:18:
                    8d:b4:01:4d:dd:99:f0:8b:42:70:64:21:69:b8:84:
                    15:04:f0:db:a9:17:fe:38:8e:4e:be:c8:b8:11:93:
                    99:0d:33:73:bc:d1:da:45:83:0b:2d:32:eb:03:ba:
                    1f:19:ff:73:5c:c0:26:20:77:1c:70:06:67:da:05:
                    3e:5a:10:f8:04:47:67:59:07:c3:f1:1c:50:0d:cf:
                    9f:1b:44:e0:a2:5e:51:47:17:7a:a7:4d:85:d5:de:
                    4b:42:43:b7:9d:dc:90:b6:7f:f2:6a:50:81:cc:4a:
                    43:57
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Subject Key Identifier:
                3A:46:CC:8E:7B:00:F1:A8:8A:54:CF:D0:BC:1A:A2:4D:F4:0E:C3:BB
            X509v3 Authority Key Identifier:
                keyid:31:5E:EC:D0:41:B3:76:6D:6C:08:C5:95:49:42:B0:D2:9F:1D:E6:2
7

    Signature Algorithm: sha1WithRSAEncryption
         0a:f5:65:8f:1e:ea:1b:5a:8e:00:ea:0c:55:73:85:a1:b1:96:
         a8:a8:b6:06:05:11:cc:39:03:ea:d6:2d:c7:cd:78:b5:a1:f6:
         79:f0:df:0d:2f:72:68:64:8a:45:46:7c:74:44:4f:b3:db:5f:
```

```
         35:a3:56:d2:92:de:0f:0f:55:ab:e2:fa:d7:33:77:7f:fd:f9:
         67:ca:3a:a4:2e:f8:40:15:4a:97:9c:a0:66:68:56:5a:70:65:
         92:bf:b4:7a:d7:5b:fc:04:55:9a:57:96:4b:41:e1:d9:03:5e:
         3e:f6:fe:4b:04:1a:8d:30:d6:c0:92:e6:44:4b:0a:37:9d:c3:
         57:bf:af:13:47:26:60:b2:6e:19:04:46:a4:dc:99:69:73:52:
         b3:1b:b6:40:45:af:f3:d3:e8:9b:3d:d9:ed:eb:b4:a8:b8:34:
         28:a9:8c:02:df:83:af:36:a0:39:b8:2f:c0:b2:bd:c0:15:d0:
         c2:09:a4:9a:f3:3f:83:21:07:cd:7d:48:c6:ac:aa:b6:8f:03:
         f8:1b:15:03:e0:c1:19:35:c9:4f:75:f5:27:99:42:06:b9:d5:
         9e:42:6a:a7:b2:2b:45:32:17:ae:f4:83:e2:14:bf:f2:d3:04:
         ef:aa:a6:92:2d:33:f0:38:a4:bc:fd:e9:d6:64:b6:e2:40:17:
         3e:6b:6a:ad

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: DC=org, DC=simple, O=Simple Inc, OU=Simple Root CA, CN=Simple Ro
ot CA
        Validity
            Not Before: Nov 27 05:03:27 2020 GMT
            Not After : Nov 27 05:03:27 2030 GMT
        Subject: DC=org, DC=simple, O=Simple Inc, OU=Simple Root CA, CN=Simple R
oot CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d5:f6:4d:18:1a:0d:fe:12:0e:3d:04:d3:c3:4f:
                    a1:6a:f6:7c:a8:56:3d:a5:95:b9:e0:d9:e4:e4:2a:
                    9e:be:ba:43:aa:c3:00:69:3e:c0:cb:f7:b3:d9:48:
                    be:3e:2d:18:a6:bf:f4:b3:85:9e:46:07:dd:22:ee:
                    61:56:78:70:76:de:e6:85:62:8c:7b:ef:c0:0d:1d:
                    23:a9:22:8e:c6:74:41:a9:90:3e:6d:0c:5e:ef:43:
                    5d:e4:3a:e7:fa:e1:7a:15:db:05:a4:3b:d4:09:c1:
                    1a:6e:f4:95:92:e8:c1:e4:81:e2:fa:a9:67:24:0f:
                    23:a4:70:77:c5:dd:9b:2f:62:8c:6c:b5:08:4b:80:
                    0d:2a:26:d0:b8:7f:a7:82:b2:da:72:48:25:55:29:
                    b1:93:d5:aa:c3:09:df:4f:83:e6:5d:b7:c6:53:b7:
                    9e:46:9d:b9:4f:60:aa:9e:e0:be:ae:f9:d4:61:26:
                    1c:e3:ac:0f:00:95:97:b4:7b:04:74:74:83:2d:23:
                    7f:44:73:7b:80:3b:7a:88:02:78:6f:c1:85:c0:e2:
                    2a:ed:c5:e1:1f:af:c0:cf:51:dd:99:f5:33:19:a3:
                    4a:99:f1:cc:6e:2d:58:7b:21:29:c3:00:4b:a0:4b:
                    8d:39:41:d5:73:31:85:45:1a:68:b4:da:1a:49:23:
                    d3:e5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
```

```
                CA:TRUE
            X509v3 Subject Key Identifier:
                31:5E:EC:D0:41:B3:76:6D:6C:08:C5:95:49:42:B0:D2:9F:1D:E6:27
            X509v3 Authority Key Identifier:
                keyid:31:5E:EC:D0:41:B3:76:6D:6C:08:C5:95:49:42:B0:D2:9F:1D:E6:2
7

    Signature Algorithm: sha1WithRSAEncryption
         80:84:36:b6:f1:ba:c3:f4:1a:59:fd:30:a2:a4:41:28:39:bd:
         4e:e2:57:07:6f:90:f8:21:c5:d1:ff:5e:12:ee:fe:43:87:b3:
         2b:50:f2:2d:5e:2a:e7:90:55:fc:aa:b5:6f:0c:0d:62:f9:3d:
         c0:ab:46:7d:6f:3c:cd:29:e4:6b:b0:d6:3f:73:56:77:bb:97:
         b3:30:04:11:1d:c1:4a:e8:00:d9:96:0f:49:4d:22:8a:00:ed:
         ca:15:bf:17:77:d1:f7:f3:df:43:ec:3f:db:5e:a5:8c:5a:4a:
         65:28:59:f4:a6:f8:77:ad:ec:90:46:cf:1c:8d:52:34:db:8d:
         d1:ee:76:cf:35:9a:22:a9:79:3c:94:04:59:09:66:49:7b:78:
         6c:a6:44:94:c3:b9:74:15:0e:7e:85:7c:1d:0c:e1:b4:56:61:
         8c:b4:e5:f8:ce:ea:f8:b0:ef:82:ba:2c:59:fe:f0:2a:c6:e9:
         e2:14:21:cf:72:86:b3:15:9f:6d:cb:5f:d2:eb:aa:66:ab:a6:
         fe:bc:cf:7f:09:0e:87:dc:d6:8a:a0:c0:5a:73:d8:d8:57:a5:
         61:c4:e0:df:13:cb:ef:5a:4d:d4:2c:38:16:e1:60:d7:98:06:
         bc:dc:7a:9d:f7:cc:29:e8:ca:8c:97:e5:72:fb:15:85:37:02:
         ed:38:13:d8

haduong@Has-MacBook-Air pki-example-1 % openssl pkcs12 \
    -in certs/fred.p12 \
    -nodes \
    -info
Enter Import Password:
MAC Iteration 2048
MAC verified OK
PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 2048
Certificate bag
Bag Attributes
    localKeyID: 2E 61 78 C4 57 4A 3B 8F 46 C3 F8 28 D3 94 F5 A9 5F F8 DC A4
    friendlyName: Fred Flintstone
subject=/DC=org/DC=simple/O=Simple Inc/CN=Fred Flintstone
issuer=/DC=org/DC=simple/O=Simple Inc/OU=Simple Signing CA/CN=Simple Signing CA
-----BEGIN CERTIFICATE-----
MIID6zCCAtOgAwIBAgIBATANBgkqhkiG9w0BAQUFADB6MRMwEQYKCZImiZPyLGQB
GRYDb3JnMRYwFAYKCZImiZPyLGQBGRYGc2ltcGxlMRMwEQYDVQQKDApTaW1wbGUg
SW5jMRowGAYDVQQLDBFTaW1wbGUgU2lnbmluZyBDQTEaMBgGA1UEAwwRU2ltcGxl
IFNpZ25pbmcgQ0EwHhcNMjAxMTI3MDUwNzI3WhcNMjIxMTI3MDUwNzI3WjBcMRMw
EQYKCZImiZPyLGQBGRYDb3JnMRYwFAYKCZImiZPyLGQBGRYGc2ltcGxlMRMwEQYD
VQQKDApTaW1wbGUgSW5jMRgwFgYDVQQDDA9GcmVkIEZsaW50c3RvbmUwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC4u2Yu+iOBL79fNZFwn6ydlP0hTmYk
e7F1xV3EJgWve7bCbo5CX3pJYItVOeB7Lz5hJ19eDO9e8RXHTOIh9oCM/y5pPuAO
expjLWhmLocX/2A91RJHSkHbVQ+n4c8cMlvIr8p9BBEB+up6fKQ9rJDA04YneB8/
ha/kAPfgbfng63ID03sOzBCYE4XxvYWeZtRPPJnLacUnBJCXXBf2ryaTh/+AjPHd
p25QNebx3EYvtr4bnRSnPEVKUOfxToGchrJbfuuYdvAVyeYlDkuL91MH2sTe9ki0
FP7xTliiVd4kNfA9G1pucMLAjQ0RF44p8HHBqFFAgw5Bof5Yli5xpI2RAgMBAAGj
gZkwgZYwDgYDVR0PAQH/BAQDAgWgMAkGA1UdEwQCMAAwHQYDVR0lBBYwFAYIKwYB
```

```
BQUHAwQGCCsGAQUFBwMCMB0GA1UdDgQWBBTAZ0gWhrNzwl9vMPj6KxxZtkcuXTAf
BgNVHSMEGDAWgBQ6RsyOewDxqIpUz9C8GqJN9A7DuzAaBgNVHREEEzARgQ9mcmVk
QHNpbXBsZS5vcmcwDQYJKoZIhvcNAQEFBQADggEBALQLceknLBdBMUayq2UMU+Su
AZ+w5J04F3/O8mOwx4fzdiIEfqyFK71nk0+6SWTWaIPhLVT9VMRwyLAcPj7EM1DG
QBlwRQV5jYKBmy/BjK2XquRIWeFW0dZbN5cvVcFP9ryHO84qapVotKteSWLisjLZ
U6eBtlOksyS12uXfevOXQ9Q6oDFn7Mr3LEI0/Qd0A9Xo6NJsUpJEbHYkoVv7VnFq
cLYm1RtFsx44csxEHpTlc3vHhK9gCwAWSeY6qg3OOT3sCgxVx6RDWURaJ8Gc9phy
silhoTBSIbgymr/oyOU4HDiafNGI7pgq0+exsk7RBC7BbZTmFpY2gsUUfjP8pLA=
-----END CERTIFICATE-----
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
Bag Attributes
    localKeyID: 2E 61 78 C4 57 4A 3B 8F 46 C3 F8 28 D3 94 F5 A9 5F F8 DC A4
    friendlyName: Fred Flintstone
Key Attributes: <No Attributes>
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC4u2Yu+iOBL79f
NZFwn6ydlP0hTmYke7F1xV3EJgWve7bCbo5CX3pJYItVOeB7Lz5hJ19eDO9e8RXH
TOIh9oCM/y5pPuAOexpjLWhmLocX/2A91RJHSkHbVQ+n4c8cMlvIr8p9BBEB+up6
fKQ9rJDA04YneB8/ha/kAPfgbfng63ID03sOzBCYE4XxvYWeZtRPPJnLacUnBJCX
XBf2ryaTh/+AjPHdp25QNebx3EYvtr4bnRSnPEVKUOfxToGchrJbfuuYdvAVyeYl
DkuL91MH2sTe9ki0FP7xTliiVd4kNfA9G1pucMLAjQ0RF44p8HHBqFFAgw5Bof5Y
li5xpI2RAgMBAAECggEAQkQO+qkGFXBgULHxkxnkHL72Mn1iDJJGbT24TgVporJZ
M9PeuhZv0mSMdq0FRosC8GzkO+Od9ku7CTweHhrDsFBVgLFqRCeKpqsCOS1Vjpkw
F94X6XTMvPX9YLaSycWSwSG2HDRaOYCdngSaEfmWD2WRSRVA+FNnbf2e7WXl7fVL
ZnIqejJaGXKwOpZ0uhwTi9tjdaNbsGxZe9gdNFuI6SqFAJ8bgsgKrCLqGkZuqCvZ
jK9E9yl+NshLd82phC2yTAxGtTW8ngexM9/qhTLH8pAAX2rRnr9PPVIF96FWyjc/
J+N3dQAvEZYX4rp0ngAiz7DtUPe2/YTipD5ZJC34RQKBgQDfC9A0qsgJoND/6o7B
aAnscv3hfbXHdBf1ctxIPrkqp7It9tqeS2LbkZ5/La/GhoYORnEs06R9YutH2nAD
/UygOwMfHAnOPLBJ6+0YEtdZi4LFGeReh/oXEkmiYTCkGwDVY1156mNxrXLk+KOh
zRpi8cCLkyyG/jk/t1Hxe7yHEwKBgQDUBnIvT99C3vIvSmVRtCNenxGcxlPVaQzA
r/Fo2gw03Ysom708ed6Wrz3nAeZ4KZI80AMKke94MK1qr7kMn7m2M3JfBSCoUwlk
sRNd/sSOWgKHTmJBtNVxLiNlL7J64zEl4U2XmFI5b6ZaZVQfUf4yyvFPriHxldf3
u5jr0Ut5SwKBgHyamOITVlUqpheR7dZWTNTvGK3UEK0wSgIw/KbPg5o0vPG4qkEs
VDndi/H4j+4UUOfAqpEkWwxBKrelbFaONzR8Qy4p98BjXwis6HM+c1fu/EsoP9Af
nrMs4D36lbXX8AtFy37EVnG3OCx6Ss+lSUxlSe+vdHyloU3bF8gUHCpJAoGBAJ3q
nyk16Ce6Pc+TLZuI+78B4vBNlysgLutlH/zkSqslRvxb4rokWvEIXKat96YP8Gdy
1pEM2LtAJimL79vDK2LVNp4nB4fXMOvaJ36evm74A2Ibs3sU4NSHdL1spRZ6GKUK
Beye+r7ktZYmWl1piFb0aH7cR1PUMyLEisU5AWm5AoGAAT/F6tmU9xG7H+uzCQ/Q
MtGsza7/Y6hE85+O+1mlsAcYYoW72ADkRz5qeQIL7mckwCjsZs3mTVlu2Oh3A9ZA
RwdTNH5HeyfAI4gYPpZkzlKl8fiDf7kNYtm6wNZvgegeDw/rAhElW77+1QdD6aUT
Z226oYMlcePr78xrcdey7tA=
-----END PRIVATE KEY-----
haduong@Has-MacBook-Air pki-example-1 % history > PKI.log
haduong@Has-MacBook-Air pki-example-1 %
```