

ca.cnf:

```
[ req ]
default_bits = 2048

prompt = no
distinguished_name=req_distinguished_name
req_extensions = v3_req

[ req_distinguished_name ]
countryName=UA
stateOrProvinceName=root region
localityName=root city
organizationName=Market(localhost)
organizationalUnitName=roote department
commonName=market.localhost
emailAddress=root_email@root.localhost

[ alternate_names ]
DNS.1      = market.localhost
DNS.2      = www.market.localhost
DNS.3      = mail.market.localhost
DNS.4      = ftp.market.localhost
DNS.5      = *.market.localhost

[ v3_req ]
keyUsage=digitalSignature
basicConstraints=CA:true
subjectKeyIdentifier = hash
subjectAltName = @alternate_names
```

child.cnf:

```
[ req ]
default_bits = 2048










prompt = no
distinguished_name=req_distinguished_name
req_extensions = v3_req

[ req_distinguished_name ]
countryName=US
stateOrProvinceName=Illinois
localityName=Peoria
organizationName=Market(localhost)
organizationalUnitName=roote department
commonName=JacksonLowder
emailAddress=jlowder@mail.bradley.edu

[ alternate_names ]
DNS.1      = market.localhost
DNS.2      = www.market.localhost
DNS.3      = mail.market.localhost
DNS.4      = ftp.market.localhost
DNS.5      = *.market.localhost

[ v3_req ]
keyUsage=digitalSignature
basicConstraints=CA:true
subjectKeyIdentifier = hash
subjectAltName = @alternate_names
```

Directory:

 ca.cnf	11/15/2023 9:41 AM	CNF File	1 KB
 child.cnf	11/15/2023 9:50 AM	CNF File	1 KB
 child.cnf.bak	11/15/2023 9:41 AM	BAK File	1 KB
 child	11/15/2023 9:50 AM	Security Certificate	2 KB
 child.csr	11/15/2023 9:50 AM	CSR File	2 KB
 child.key	11/15/2023 9:50 AM	KEY File	2 KB
 rootCA.key	11/15/2023 9:50 AM	KEY File	2 KB
 rootCA.pem	11/15/2023 9:50 AM	PEM File	2 KB
 rootCA.srl	11/15/2023 9:50 AM	SRL File	1 KB

```
C:\Users\jacks\Desktop\OpenSSL_Assignment>openssl x509 -req -in child.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out child.crt -days 365 -sha256 -extfile child.cnf
Certificate request self-signature ok
subject=C = US, ST = Illinois, L = Peoria, O = Market(localhost), OU = roote department, CN = JacksonLowder, emailAddress = jlowder@mail.bradley.edu

C:\Users\jacks\Desktop\OpenSSL_Assignment>openssl x509 -in child.crt -text -noout
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            46:83:02:eb:bd:72:46:a4:7e:7b:e7:1d:ae:5e:86:d8:2c:40:f1:50
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = UA, ST = root region, L = root city, O = Market(localhost), OU = roote department, CN = market.localhost, emailAddress = root_email@root.localhost
        Validity
            Not Before: Nov 15 15:50:41 2023 GMT
            Not After : Nov 14 15:50:41 2024 GMT
        Subject: C = US, ST = Illinois, L = Peoria, O = Market(localhost), OU = roote department, CN = JacksonLowder, emailAddress = jlowder@mail.bradley.edu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:e3:a6:6b:8f:08:2a:f1:8e:9c:69:ec:0f:46:b5:
                a9:2e:82:cf:33:64:9e:3d:06:c0:f5:c0:05:7c:7c:
                8d:1b:d0:78:50:2e:9c:16:b3:2b:90:fb:b7:58:fc:
                51:6f:22:e8:e3:8d:61:19:15:42:fe:ef:98:d7:0f:
                d4:80:af:b0:07:88:81:3a:9f:85:0c:cc:a9:72:e8:
                a4:75:3e:ec:63:a9:e4:d1:7d:bd:53:ee:11:63:a3:
                f5:19:37:3e:4a:d5:b1:20:6d:89:4b:8e:9a:20:d6:
                f6:f1:c9:d5:5c:63:07:ef:7f:5d:63:02:0a:f4:d2:
                cd:73:dc:52:b5:c3:2b:75:c1:33:1e:24:54:3f:e2:
                88:4e:a7:c6:06:9c:64:18:61:18:ee:53:30:01:94:
                90:69:07:04:bc:bb:a6:36:87:2d:87:bf:99:d6:6c:
                de:83:e5:51:dd:05:42:b1:d0:0a:4b:df:86:2f:68:
                03:7d:16:9f:1e:cb:3c:0e:ab:35:b1:64:b9:b8:c8:
                65:0a:2f:b5:72:39:32:dc:df:72:26:5b:d0:d0:62:
                ac:25:49:66:c0:4f:de:b4:ca:38:87:e8:26:00:d0:
                6c:ba:b7:d7:9a:0e:1c:f7:bf:4b:be:6f:97:22:45:
                7d:d2:e1:a5:83:ca:07:07:f3:48:21:39:52:29:90:
                35:fb
            Exponent: 65537 (0x10001)
        Signature Algorithm: sha256WithRSAEncryption
        Signature Value:
            4c:07:ba:d6:2f:12:29:d9:88:62:db:56:df:13:22:44:90:6a:
            cc:40:13:af:2d:75:6f:43:44:94:2a:f0:b0:e6:73:ae:c0:ee:
            28:36:e7:3d:c0:e2:81:74:d3:14:81:dd:4f:4a:73:a9:f3:88:
            65:a6:19:ce:44:cb:c0:50:91:c0:a0:b1:b7:74:a7:60:bc:56:
            8b:ea:be:8d:1c:1c:21:f0:e2:58:99:57:6b:59:44:d8:87:cf:
            77:aa:ea:bd:07:f1:aa:e4:f4:e9:a9:8f:32:59:68:cd:ab:e9:
            4e:4b:b4:8e:6f:ac:9a:bd:e2:c7:c7:8f:54:d3:9e:38:92:a8:
            0f:f3:c9:de:f2:81:4e:a2:67:e4:2d:14:05:9e:a2:81:89:71:
            d0:a7:1e:39:e8:70:dc:00:bb:44:b2:19:d3:45:d5:e4:59:0d:
            3e:d9:02:c8:46:59:a4:1b:b2:bb:d2:07:88:7b:da:f2:f4:9a:
            e9:ea:b9:4e:9c:b9:16:17:2c:77:64:b8:82:a4:d9:8d:f5:2f:
            67:f9:2b:2d:08:49:cb:1a:0e:7a:5d:f6:69:ff:4b:ff:b0:0e:
            4e:41:dc:68:cd:df:13:4c:4b:1b:ea:5f:35:e4:cf:0d:28:70:
            ff:2b:1d:b2:4d:78:8d:97:ab:6f:7e:6f:91:da:70:0f:6c:6f:
            31:59:84:c1

C:\Users\jacks\Desktop\OpenSSL_Assignment>
```

Commands Used:

- openssl genrsa -out rootCA.key 2048
- openssl req -x509 -new -nodes -key rootCA.key -days 1024 -out rootCA.pem -config ca.cnf
- openssl genrsa -out child.key 2048
- openssl req -new -key child.key -out child.csr -config child.cnf
- openssl x509 -req -in child.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out child.crt -days 365 -sha256 -extfile child.cnf
- openssl x509 -in child.crt -text -noout

Extra Credit:**1. Subject Alternative Name (SAN):**

```
[ v3_req ]
```

```
...
```

```
subjectAltName = @alt_names
```

```
[ alt_names ]
```

```
DNS.1 = example.com
```

```
DNS.2 = www.example.com
```

This extension allows the certificate to be valid for multiple names or IP addresses. It's crucial for certificates used in web servers that need to be valid for multiple domain names or subdomains.

2. Key Usage:

```
[ v3_req ]
```

```
...
```

```
keyUsage = digitalSignature, keyEncipherment
```

This extension defines the purpose of the public key contained in the certificate (e.g., for digital signatures, key encipherment).

3. Extended Key Usage:

[v3_req]

...

extendedKeyUsage = serverAuth, clientAuth

This specifies more precisely the application contexts where the certificate's public key can be used (e.g., for server authentication, client authentication).

4. Basic Constraints:

[v3_req]

...

basicConstraints = CA:FALSE

This extension indicates whether a certificate is a CA certificate. It's crucial for intermediate certificates.

5. Certificate Policies:

[v3_req]

...

certificatePolicies = @cert_policies

[cert_policies]

policyIdentifier = 1.2.3.4.5.6.7

CPS.1 = <http://www.example.com/cps>

This extension includes a list of policy information terms to indicate the policy under which the certificate has been issued.