eDirectory PKI Server Cookbook

Table of Contents

In this document, I plan to capture various use cases around eDirectory Certificate Server, eDirectory server certificates and troubleshooting tips. This is intended to be a live document which will get updated with more information over time.

How to examine eDirectory CA certificate

eDirectory versions 9.0 and later have two CAs - a RSA CA and a ECDSA CA.

```
bash$ ls -1 /var/opt/novell/eDirectory/data/*.pem
/var/opt/novell/eDirectory/data/SSCert.pem
/var/opt/novell/eDirectory/data/SSECCert.pem
```

RSA CA certificate

EC CA certificate

tree name

These certificates are present in my eDirectory tree as attributes of the object:
`cn=TEST-TREE-1 CA,cn=Security`
and are made available here for convenience.
The certificate can be examined as follows:

```
bash$ openssl x509 -text -in /var/opt/novell/eDirectory/data/SSCert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            7f:65:c6:23:a2:3d:cd:a0:5f:b4:0f:85:53:1d:9e:5a:a2:b7:f0:c0
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: OU=Organizational CA, O=TEST-TREE-1
        Validity
            Not Before: Dec 13 12:34:07 2018 GMT
            Not After : Dec 12 12:34:07 2028 GMT
        Subject: OU=Organizational CA, O=TEST-TREE-1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:f5:a9:bc:d1:43:83:11:7e:44:bf:0b:9a:77:31:
                    a0:01:45:41:15:fb:49:f9:83:89:2e:bf:4a:b3:f3:
```

if issuer and subject are same, it is called a *self signed certificate*.

these two times indicate the certificate validity period. Make sure current time is between them.

```
                    d1:bb:27:71:5f:c3:b8:98:14:07:33:7c:5c:f8:b4:
                    bb:8d:1d:9f:a1:e3:09:22:ff:d3:11:b5:c2:03:dc:
                    c6:a6:3e:c9:5a:a1:ab:b0:f5:65:2a:5f:04:e2:e4:
                    b0:3d:f1:3c:61:e6:7f:26:f4:b3:33:61:0e:07:23:
                    fd:31:00:d6:fd:19:ff:b9:70:4b:56:88:23:08:8e:
                    ff:6c:6a:5b:23:c1:57:7f:b3:03:d7:55:df:71:f8:
                    ca:5a:44:b6:4d:67:74:b6:f1:d3:63:07:f3:cf:ef:
                    7a:31:23:c0:ac:e1:35:9b:62:84:14:4a:44:e4:9b:
                    19:5e:fe:65:ff:af:0c:28:8c:cb:58:1d:72:c8:ea:
                    b8:10:2f:ce:72:0e:89:5b:31:4c:ed:99:e9:4e:f5:
                    ad:d8:89:83:74:21:8a:2f:27:85:7f:9e:9c:49:19:
                    e5:4f:d2:1d:d2:3e:9f:d2:67:02:e6:9b:9f:0b:0e:
                    e0:93:fd:11:64:cd:2e:39:c8:06:0b:20:f5:1f:70:
                    b4:f1:2a:2f:78:d1:a9:71:67:a3:9b:26:b6:c6:03:
                    ae:42:77:3f:f3:a5:9e:62:31:70:02:2e:a2:a1:86:
                    15:6f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                1A:2A:3C:5B:B6:C7:B7:94:00:FE:27:77:C1:84:00:40:3B:F3:AC:2C
            X509v3 Authority Key Identifier:

keyid:1A:2A:3C:5B:B6:C7:B7:94:00:FE:27:77:C1:84:00:40:3B:F3:AC:2C

            X509v3 Basic Constraints:
                CA:TRUE
            X509v3 Key Usage:
                Certificate Sign, CRL Sign
            2.16.840.1.113719.1.9.4.1:
                0...........Novell Security
Attribute(tm).Chttp://developer.novell.com/repository/attributes/certattrs_v10.
htm0..H.....0.0......F0.0......
.......................0.0.................0.0............................NO
L...........
    Signature Algorithm: sha256WithRSAEncryption
         95:a6:cd:4a:66:ca:c7:f0:a8:18:21:dd:3c:d6:ef:65:41:cc:
         80:3f:66:79:48:c5:75:36:bb:37:d3:52:84:3e:53:25:31:b6:
         9b:b1:c9:df:f0:f0:5b:3d:cb:a4:78:b7:2e:09:25:b0:b5:19:
         d7:31:e5:eb:7e:36:7a:ac:cd:49:52:5d:d3:6c:9e:ac:05:5b:
         74:4e:15:69:ba:2c:23:57:26:51:b4:a3:7f:5d:76:86:8f:b0:
         58:09:0b:7a:12:53:e2:08:80:80:a2:75:b6:a6:fe:6e:9f:ff:
         56:b9:ea:81:f0:56:5f:78:81:ce:9d:b3:46:6e:4d:28:19:65:
```

```
        23:59:a4:f9:39:61:34:c3:a5:5e:25:a5:1f:d3:1e:9e:c7:8a:
        9e:87:c0:a7:fd:d7:b8:0d:6b:b7:27:08:ff:07:b1:86:7f:cf:
        72:15:3a:ed:51:78:b1:05:1e:83:78:1d:41:61:51:e3:94:d2:
        a3:68:c7:60:26:6c:09:71:a6:d6:ef:13:91:0a:f6:77:3a:f2:
        a8:6b:85:5c:78:cc:b4:ff:e0:54:7e:2a:80:a8:3f:a0:9f:16:
        26:0f:82:16:52:af:44:b9:4e:d7:3a:56:86:a0:61:7c:89:11:
        da:5d:e8:31:df:d1:99:0e:4e:1e:67:25:5c:90:40:1a:5f:43:
        bb:bf:c0:87
-----BEGIN CERTIFICATE-----
MIIFIzCCBAugAwIBAgIUf2XGI6I9zaBftA+FUx2eWqK38MAwDQYJKoZIhvcNAQEL
BQAwMjEaMBgGA1UECxMRT3JnYW5pemF0aW9uYWwgQ0ExFDASBgNVBAoTC1RFU1Qt
VFJFRS0xMB4XDTE4MTIxMzEyMzQwN1oXDTI4MTIxMjEyMzQwN1owMjEaMBgGA1UE
CxMRT3JnYW5pemF0aW9uYWwgQ0ExFDASBgNVBAoTC1RFU1QtVFJFRS0xMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA9am8OUODEX5EvwuadzGgAUVBFftJ
+YOJLr9Ks/PRuydxX8O4mBQHM3xc+LS7jR2foeMJIv/TEbXCA9zGpj7JWqGrsPVl
Kl8E4uSwPfE8YeZ/JvSzM2EOByP9MQDW/Rn/uXBLVogjCI7/bGpbI8FXf7MD11Xf
cfjKWkS2TWd0tvHTYwfzz+96MSPArOE1m2KEFEpE5JsZXv5l/68MKIzLWB1yyOq4
EC/Ocg6JWzFM7ZnpTvWt2ImDdCGKLyeFf56cSRnlT9Id0j6f0mcC5pufCw7gk/0R
ZM0uOcgGCyD1H3C08SoveNGpcWejmya2xgOuQnc/86WeYjFwAi6ioYYVbwIDAQAB
o4ICLzCCAiswHQYDVR0OBBYEFBoqPFu2x7eUAP4nd8GEAEA786wsMB8GA1UdIwQY
MBaAFBoqPFu2x7eUAP4nd8GEAEA786wsMAwGA1UdEwQFMAMBAf8wCwYDVR0PBAQD
AgEGMIIBzAYLYIZIAYb4NwEJBAEEggG7MIIBtwQCAQABAf8THU5vdmVsbCBTZWN1
cml0eSBBdHRyaWJ1dGUodG0pFkNodHRwOi8vZGV2ZWxvcGVyLm5vdmVsbC5jb20v
cmVwb3NpdG9yeS9hdHRyaWJ1dGVzL2NlcnRhdHRyc192MTAuaHRtMIIBSKAaAQEA
MAgwBgIBAQIBRjAIMAYCAQECAQoCAWmhGgEBADAIMAYCAQECAQAwCDAGAgEBAgEA
AgEAogYCARgBAf+jggEEoFgCAQICAgD/AgEAAw0AgAAAAAAAAAAAAAAAwkAgAAA
AAAAAAAwGDAQAgEAAgh/////////wEBAAIEBvDfSDAYMBACAQACCH/////////
AQEAAgQG8N9IoVgCAQICAgD/AgEAAw0AQAAAAAAAAAAAAAAAAwkAQAAAAAAAAAAw
GDAQAgEAAgh/////////wEBAAIEEf+ugTAYMBACAQACCH/////////AQEAAgQR
/66Bok4wTAIBAgICAP8CAQADDQCA/////////////8DCQCA////////zASMBAC
AQACCH/////////AQH/MBIwEAIBAAIIf////////8BAf8wDQYJKoZIhvcNAQEL
BQADggEBAJWmzUpmysfwqBgh3TzW72VBzIA/ZnlIxXU2uzfTUoQ+UyUxtpuxyd/w
8Fs9y6R4ty4JJbC1Gdcx5et+NnqszUlSXdNsnqwFW3ROFWm6LCNXJlGOo39ddoaP
sFgJC3oSU+IIgICidbam/m6f/1a56oHwVl94gc6ds0ZuTSgZZSNZpPk5YTTDpV4l
pR/THp7Hip6HwKf917gNa7cnCP8HsYZ/z3IVOu1ReLEFHoN4HUFhUeOU0qNox2Am
bAlxptbvE5EK9nc68qhrhVx4zLT/4FR+KoCoP6CfFiYPghZSr0S5Ttc6VoagYXyJ
Edpd6DHf0ZkOTh5nJVyQQBpfQ7u/wIc=
-----END CERTIFICATE-----
```

this is the actual base64 encoded certificate stored in the .pem file

How to examine eDirectory server certificate

Note: For the following commands to work, run `export LDAPTLS_REQCERT=never` in the shell before executing the commands.

Server certificates are stored in eDirectory objects called Key Material Objects (KMOs). Following is how you locate the KMO.

```
bash$ ldapsearch -H ldaps://127.0.0.1 -b '' -s base dsaName -x -LLL
dn:
dsaName: cn=m1,o=novell
bash$ ldapsearch -H ldaps://127.0.0.1 -b 'cn=m1,o=novell' -s base ldapServerDN
-D cn=admin,o=novell -x -LLL
dn: cn=m1,o=novell
ldapServerDN: cn=LDAP Server - m1,o=novell
bash$ ldapsearch -H ldaps://127.0.0.1 -b 'cn=LDAP Server - m1,o=novell' -s base
ldapKeyMaterialName -D cn=admin,o=novell -x -LLL
dn: cn=LDAP Server - m1,o=novell
ldapKeyMaterialName: SSL CertificateDNS
```

this is the local DSA's DN

This is LDAP server's DN

this means that the KMO DN is `cn=SSL CertificateDNS - m1,o=novell`

LDAP server certificate contents

You can use the following command to see the LDAP server's X509 certificate.

```
bash$ openssl s_client -showcerts -connect 127.0.0.1:636
CONNECTED(00000003)
depth=1 OU = Organizational CA, O = TEST-TREE-1
verify error:num=19:self signed certificate in certificate chain
---
Certificate chain
 0 s:/O=TEST-TREE-1/CN=m1.foo.com
   i:/OU=Organizational CA/O=TEST-TREE-1
-----BEGIN CERTIFICATE-----
MIIGvzCCBaegAwIBAgIUNQ0fNpmSeuj4GcMDl8wYKF2ZYpwwDQYJKoZIhvcNAQEL
BQAwMjEaMBgGA1UECxMRT3JnYW5pemF0aW9uYWwgQ0ExFDASBgNVBAoTC1RFU1Qt
VFJFRS0xMB4XDTE4MTIxNTEwMzQwOFoXDTIwMTIxNDEwMzQwOFowKzEUMBIGA1UE
ChMLVEVTVC1UUkVFLTExEzARBgNVBAMTCm0xLmZvby5jb20wggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQCvemycNaO6CI+hItGZBw4qzPqHCvqHijkyjfCf
GUOAWz4Y+w4jVgVFaFU3J9SiBgv7KtBRf9kAhHH8Um3TGgEuucxMqd7xFGnYIhom
pMS8Mnot77Ya4mQNvY/ShnaDnvdUMfaMkBNnTF56e4gNW1YWtz2WhfLwgxR91aug
wxxNiG2AZ6St2qMXjXwWk4XjUD9v/vTQRXddbhdbxgoBXqdsTQBKBmrlJYgqgVJs
fYHo/YqoVun/ggcRxkithXnup9IDE1twsJAFXrlO5VVfEZNstUsIWW9U/xBOQeHL
TpIePE1dl763Y8Ir7AKSL8jJDfyPala65q+4CSAx+E89bzd/AgMBAAGjggPSMIID
zjAdBgNVHQ4EFgQUA/Bfib9lvx72tvq0EYsmP2o5xUcwHwYDVR0jBBgwFoAUGio8
W7bHt5QA/id3wYQAQDvzrCwwGwYDVR0RBBQwEocEwKg4ZoIKbTEuZm9vLmNvbTAL
BgNVHQ8EBAMCBaAwggHMBgtghkgBhvg3AQkEAQSCAbswggG3BAIBAAEB/xMdTm92
ZWxsIFNlY3VyaXR5IEF0dHJpYnV0ZSh0bSkWQ2h0dHA6Ly9kZXZlbG9wZXIubm92
ZWxsLmNvbS9yZXBvc2l0b3J5L2F0dHJpYnV0ZXMvY2VydGF0dHJzX3YxMC5odG0w
ggFIoBoBAQAwCDAGAgEBAgFGMAgwBgIBAQIBCgIBaaEaAQEAMAgwBgIBAQIBADAI
```

Certificate subject name contains the server's DNS name. So, the following certificate is the LDAP server's certificate

copy/paste this into file `server-cert.pem` for examining

```
MAYCAQECAQACAQCiBgIBFwEB/6OCAQSgWAIBAgICAP8CAQADDQCAAAAAAAAAAAA
AAADCQCAAAAAAAAAADAYMBACAQACCH/////////AQEAAgQG8N9IMBgwEAIBAAII
f/////////8BAQACBAbw30ihWAIBAgICAP8CAQADDQBAAAAAAAAAAAAAAADCQBA
AAAAAAAAADAYMBACAQACCH/////////AQEAAgQR/66BMBgwEAIBAAIIf///////
//8BAQACBBH/roGiTjBMAgECAgEAAgIA/wMNAIAAAAAAAAAAAAAAAMJAIAAAAAA
AAAAMBIwEAIBAAIIf/////////8BAQAwEjAQAgEAAgh/////////wEBADCCAZAG
A1UdHwSCAYcwggGDMCygKqAohiZodHRwOi8vMTkyLjE2OC41Ni4xMDI6ODAyOC9j
cmwvb25lLmNybDBgoF6gXIZabGRhcDovLzE5Mi4xNjguNTYuMTAyOjM4OS9DTj1P
bmUsQ049T25lJTIwLSUyMENvbmZpZ3VyYXRpb24sQ049Q1JMJTIwQ29udGFpbmVy
LENOPVNlY3VyaXR5MC2gK6AphidodHRwczovLzE5Mi4xNjguNTYuMTAyOjgwMzAv
Y3JsL29uZS5jcmwwYaBfoF2GW2xkYXBzOi8vMTkyLjE2OC41Ni4xMDI6NjM2L0NO
PU9uZSxDTj1PbmUlMjAtJTIwQ29uZmlndXJhdGlvbixDTj1DUkwlMjBDb250YWlu
ZXIsQ049U2VjdXJpdHkwX6BdoFukWTBXMQwwCgYDVQQDEwNPbmUxHDAaBgNVBAMT
E09uZSAtIENvbmZpZ3VyYXRpb24xFjAUBgNVBAMTDUNSTCBDb250YWluZXIxETAP
BgNVBAMTCFNlY3VyaXR5MA0GCSqGSIb3DQEBCwUAA4IBAQDBnJMF8o96TQGhHDaG
AKwp2QRujWk7aW2lpz1xzC0zjNA7a684OYZjJhAAHDiLuva3fFtkLGRo7VvRqwhn
jrtzq2pz6OOBBruHQqGIL67c+JYgSTI22NL8ljpn0dbEf0bHMdibcHSjY0hckIXF
NZG2TEglMwU/mnc037xBC1LAvtLXh1LnK7O2tqsrIk+LwCteyPcxWhgcQotAakKF
WjuGgqSoz6l88vrT4c4IGvxeySPCykHoTc6qeEQpBX9TtenoD/AJRIjcv6HciqrQ
U1lDdCyemNirahzZH+gEo+JkmxsvPnFIX1ptMILb3AQ7ViayvRwHr1Ldl+l7WbIt
NnPr
```

-----END CERTIFICATE-----

```
 1 s:/OU=Organizational CA/O=TEST-TREE-1
   i:/OU=Organizational CA/O=TEST-TREE-1
```

subject name and issuer name are same here. So, following is the CA certificate we saw in previous section

-----BEGIN CERTIFICATE-----

```
MIIFIzCCBAugAwIBAgIUf2XGI6I9zaBftA+FUx2eWqK38MAwDQYJKoZIhvcNAQEL
BQAwMjEaMBgGA1UECxMRT3JnYW5pemF0aW9uYWwgQ0ExFDASBgNVBAoTC1RFU1Qt
VFJFRS0xMB4XDTE4MTIxMzEyMzQwN1oXDTI4MTIxMjEyMzQwN1owMjEaMBgGA1UE
CxMRT3JnYW5pemF0aW9uYWwgQ0ExFDASBgNVBAoTC1RFU1QtVFJFRS0xMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA9am80UODEX5EvwuadzGgAUVBFftJ
+YOJLr9Ks/PRuydxX8O4mBQHM3xc+LS7jR2foeMJIv/TEbXCA9zGpj7JWqGrsPVl
Kl8E4uSwPfE8YeZ/JvSzM2EOByP9MQDW/Rn/uXBLVogjCI7/bGpbI8FXf7MD11Xf
cfjKWkS2TWd0tvHTYwfzz+96MSPArOE1m2KEFEpE5JsZXv5l/68MKIzLWB1yyOq4
EC/Ocg6JWzFM7ZnpTvWt2ImDdCGKLyeFf56cSRnlT9Id0j6f0mcC5pufCw7gk/0R
ZM0uOcgGCyD1H3C08SoveNGpcWejmya2xgOuQnc/86WeYjFwAi6ioYYVbwIDAQAB
o4ICLzCCAiswHQYDVR0OBBYEFBoqPFu2x7eUAP4nd8GEAEA786wsMB8GA1UdIwQY
MBaAFBoqPFu2x7eUAP4nd8GEAEA786wsMAwGA1UdEwQFMAMBAf8wCwYDVR0PBAQD
AgEGMIIBzAYLYIZIAYb4NwEJBAEEggG7MIIBtwQCAQABAf8THU5vdmVsbCBTZWN1
cml0eSBBdHRyaWJ1dGUodG0pFkNodHRwOi8vZGV2ZWxvcGVyLm5vdmVsbC5jb20v
cmVwb3NpdG9yeS9hdHRyaWJ1dGVzL2NlcnRhdHRyc192MTAuaHRtMIIBSKAaAQEA
MAgwBgIBAQIBRjAIMAYCAQECAQoCAWmhGgEBADAIMAYCAQECAQAwCDAGAgEBAgEA
AgEAogYCARgBAf+jggEEoFgCAQICAgD/AgEAAw0AgAAAAAAAAAAAAAAAwkAgAAA
```

```
AAAAAAAwGDAQAgEAAgh/////////wEBAAIEBvDfSDAYMBACAQACCH/////////
AQEAAgQG8N9IoVgCAQICAgD/AgEAAw0AQAAAAAAAAAAAAAAAAwkAQAAAAAAAAAw
GDAQAgEAAgh/////////wEBAAIEEf+ugTAYMBACAQACCH/////////AQEAAgQR
/66Bok4wTAIBAgICAP8CAQADDQCA//////////8DCQCA////////zASMBAC
AQACCH/////////AQH/MBIwEAIBAAIIf////////8BAf8wDQYJKoZIhvcNAQEL
BQADggEBAJWmzUpmysfwqBgh3TzW72VBzIA/ZnlIxXU2uzfTUoQ+UyUxtpuxyd/w
8Fs9y6R4ty4JJbC1Gdcx5et+NnqszUlSXdNsnqwFW3ROFWm6LCNXJlG0o39ddoaP
sFgJC3oSU+IIgICidbam/m6f/1a56oHwVl94gc6ds0ZuTSgZZSNZpPk5YTTDpV4l
pR/THp7Hip6HwKf917gNa7cnCP8HsYZ/z3IVOu1ReLEFHoN4HUFhUeOU0qNox2Am
bAlxptbvE5EK9nc68qhrhVx4zLT/4FR+KoCoP6CfFiYPghZSr0S5Ttc6VoagYXyJ
Edpd6DHf0ZkOTh5nJVyQQBpfQ7u/wIc=
-----END CERTIFICATE-----
---
Server certificate
subject=/O=TEST-TREE-1/CN=m1.foo.com
issuer=/OU=Organizational CA/O=TEST-TREE-1
---
No client certificate CA names sent
---
SSL handshake has read 3382 bytes and written 611 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : AES256-GCM-SHA384
    Session-ID:
39706288F9ED5AB4B38FE8945F11EF65F10D4D14AEDB32FB71D9FA0F576BDA4F
    Session-ID-ctx:
    Master-Key:
E1949164CE260BE467A843ADC23458FBC093B90AAF16A56F787D350EAC714CA19A49BFCD7062695
C042B1E53F759CCD6
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
```

these are the TLS version and cipher suite used for secure communication

```
    0000 - 93 38 de 7a 5d 72 54 3e-72 75 32 07 b8 e1 60 01   .8.z]rT>ru2...`.
    0010 - 4e 99 9b 68 80 29 45 d1-3f 68 9c a7 40 fd b4 ea   N..h.)E.?h..@...
    0020 - 29 5a 11 1d d7 02 81 a5-dc b0 dc d4 66 c4 9b 5d   )Z.........f..]
    0030 - 97 be 2f 84 87 29 9f 88-7c 6f 15 59 42 c9 d1 e5   ../..)..|o.YB...
    0040 - 86 07 bd cf 6f 05 fd e3-70 64 d3 b5 2f 8e 5b 06   ....o...pd../.[.
    0050 - de 10 f9 5e 39 5b 43 4c-51 39 da 85 88 79 82 29   ...^9[CLQ9...y.)
    0060 - 84 3c f1 d8 e6 0b 0a 4f-1b f3 d3 90 d0 d8 93 87   .<.....O........
    0070 - f4 38 f1 8b 3b 5b 9a 1c-6d bb bc 89 81 0d 6a 2b   .8..;[..m.....j+
    0080 - 37 16 c1 57 69 cc 05 cc-dd 6b d6 d6 d0 76 a0 da   7..Wi....k...v..
    0090 - 67 2f a6 cd 21 f0 75 37-bb 1c 77 49 73 6a bd 7c   g/..!.u7..wIsj.|
    00a0 - f5 ea 82 71 e2 ea 9f 6a-be a2 0e 40 e0 e3 8c 9a   ...q...j...@....

    Start Time: 1544952837
    Timeout   : 300 (sec)
    Verify return code: 19 (self signed certificate in certificate chain)
```

Now, examine the server certificate that you copied into server-cert.pem using the following command. The command is same as the one used to examine the CA certificate.

```
bash$ openssl x509 -text -in server-cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            35:0d:1f:36:99:92:7a:e8:f8:19:c3:03:97:cc:18:28:5d:99:62:9c
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: OU=Organizational CA, O=TEST-TREE-1
        Validity
            Not Before: Dec 15 10:34:08 2018 GMT
            Not After : Dec 14 10:34:08 2020 GMT
        Subject: O=TEST-TREE-1, CN=m1.foo.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:af:7a:6c:9c:35:a3:ba:08:8f:a1:22:d1:99:07:
                    0e:2a:cc:fa:87:0a:fa:87:8a:39:32:8d:f0:9f:19:
                    4d:00:5b:3e:18:fb:0e:23:56:05:45:68:55:37:27:
                    d4:a2:06:0b:fb:2a:d0:51:7f:d9:00:84:71:fc:52:
                    6d:d3:1a:01:2e:b9:cc:4c:a9:de:f1:14:69:d8:22:
                    1a:26:a4:c4:bc:32:7a:2d:ef:b6:1a:e2:64:0d:bd:
                    8f:d2:86:76:83:9e:f7:54:31:f6:8c:90:13:67:4c:
```

these are the start and end times of certificate validity. Make sure the current time is between them. Otherwise, authentications will fail

server's DNS name

```
                    5e:7a:7b:88:0d:5b:56:16:b7:3d:96:85:f2:f0:83:
                    14:7d:d5:ab:a0:c3:1c:4d:88:6d:80:67:a4:ad:da:
                    a3:17:8d:7c:16:93:85:e3:50:3f:6f:fe:f4:d0:45:
                    77:5d:6e:17:5b:c6:0a:01:5e:a7:6c:4d:00:4a:06:
                    6a:e5:25:88:2a:81:52:6c:7d:81:e8:fd:8a:a8:56:
                    e9:ff:82:07:11:c6:48:ad:85:79:ee:a7:d2:03:13:
                    5b:70:b0:90:05:5e:b9:4e:e5:55:5f:11:93:6c:b5:
                    4b:08:59:6f:54:ff:10:4e:41:e1:cb:4e:92:1e:3c:
                    4d:5d:97:be:b7:63:c2:2b:ec:02:92:2f:c8:c9:0d:
                    fc:8f:6a:56:ba:e6:af:b8:09:20:31:f8:4f:3d:6f:
                    37:7f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                03:F0:5F:89:BF:65:BF:1E:F6:B6:FA:B4:11:8B:26:3F:6A:39:C5:47
            X509v3 Authority Key Identifier:

keyid:1A:2A:3C:5B:B6:C7:B7:94:00:FE:27:77:C1:84:00:40:3B:F3:AC:2C
            X509v3 Subject Alternative Name:
                IP Address:192.168.56.102, DNS:m1.foo.com
            X509v3 Key Usage:
                Digital Signature, Key Encipherment
            2.16.840.1.113719.1.9.4.1:
                0.....Novell Security
Attribute(tm).Chttp://developer.novell.com/repository/attributes/certattrs_v10.
htm0..H.....0.0......F0.0......
.....0.0.....0.0.....NO
L.....
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://192.168.56.102:8028/crl/one.crl
                Full Name:
                  URI:ldap://192.168.56.102:389/CN=One,CN=One%20-
%20Configuration,CN=CRL%20Container,CN=Security
                Full Name:
                  URI:https://192.168.56.102:8030/crl/one.crl
                Full Name:
                  URI:ldaps://192.168.56.102:636/CN=One,CN=One%20-
%20Configuration,CN=CRL%20Container,CN=Security
                Full Name:
```

this is one of the most important fields. It has a list of DNS and IP addresses of server that clients connect to. If client uses any address other than these, authentication will fail

This section contains the list of URLs from which the Certificate Revocation List (CRL) can be downloaded. The TLS client would need to access these URLs.

CRL is available for download from the server configured as the PKI CA. In this case, 192.168.56.102

```
                DirName: CN = One, CN = One - Configuration, CN = CRL
Container, CN = Security
    Signature Algorithm: sha256WithRSAEncryption
         c1:9c:93:05:f2:8f:7a:4d:01:a1:1c:36:86:00:ac:29:d9:04:
         6e:8d:69:3b:69:6d:a5:a7:3d:71:cc:2d:33:8c:d0:3b:6b:af:
         38:39:86:63:26:10:00:1c:38:8b:ba:f6:b7:7c:5b:64:2c:64:
         68:ed:5b:d1:ab:08:67:8e:bb:73:ab:6a:73:e8:e3:81:06:bb:
         87:42:a1:88:2f:ae:dc:f8:96:20:49:32:36:d8:d2:fc:96:3a:
         67:d1:d6:c4:7f:46:c7:31:d8:9b:70:74:a3:63:48:5c:90:85:
         c5:35:91:b6:4c:48:25:33:05:3f:9a:77:34:df:bc:41:0b:52:
         c0:be:d2:d7:87:52:e7:2b:b3:b6:b6:ab:2b:22:4f:8b:c0:2b:
         5e:c8:f7:31:5a:18:1c:42:8b:40:6a:42:85:5a:3b:86:82:a4:
         a8:cf:a9:7c:f2:fa:d3:e1:ce:08:1a:fc:5e:c9:23:c2:ca:41:
         e8:4d:ce:aa:78:44:29:05:7f:53:b5:e9:e8:0f:f0:09:44:88:
         dc:bf:a1:dc:8a:aa:d0:53:59:43:74:2c:9e:98:d8:ab:6a:1c:
         d9:1f:e8:04:a3:e2:64:9b:1b:2f:3e:71:48:5f:5a:6d:30:82:
         db:dc:04:3b:56:26:b2:bd:1c:07:af:52:dd:97:e9:7b:59:b2:
         2d:36:73:eb
```