Seng 360 Assignment 6

[redacted]

Public Key Crypto

1. ********** **Command** **********

```
[10/20/20]seed@VM:~$ openssl s_client -connect www.td.com:443 -showcerts
CONNECTED(00000003)
depth=2 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert High Assurance EV Root CA
verify return:1
depth=1 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert SHA2 Extended Validation Server CA
verify return:1
depth=0 businessCategory = Private Organization, jurisdictionC = CA, jurisdictionST = Nova Scotia, serialNumber = 1010197, C = CA, ST = Ontario, L = Toronto, O = The Toronto-Dominion Bank, OU = TDCMB-V, CN = td.com
verify return:1
---
Certificate chain
 0 s:/businessCategory=Private Organization/jurisdictionC=CA/jurisdictionST=Nova Scotia/serialNumber=1010197/C=CA/ST=Ontario/L=Toronto/O=The Toronto-Dominion Bank/OU=TDCMB-V/CN=td.com
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended Validation Server CA
-----BEGIN CERTIFICATE-----
MIIHSzCCBjOgAwIBAgIQB9gt165ngvgCSAaF425BXzANBgkqhkiG9w0BAQsFADB1
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMTQwMgYDVQQDEytEaWdpQ2VydCBTSEEyIEV4dGVuZGVk
IFZhbGlkYXRpb24gU2VydmVyIENBMB4XDTE5MDUxNTAwMDAwMFoXDTIxMDExMTEy
MDAwMFowgdwxHTAbBgNVBA8MFFByaXZhdGUgT3JnYW5pemF0aW9uMRMwEQYLKwYB
BAGCNzwCAQMTAkNBMRwwGgYLKwYBBAGCNzwCAQITC05vdmEgU2NvdGlhMRAwDgYD
VQQFEwcxMDEwMTk3MQswCQYDVQQGEwJDQTEQMA4GA1UECBMHT250YXJpbzEQMA4G
A1UEBxMHVG9yb250bzEiMCAGA1UEChMZVGhlIFRvcm9udG8tRG9taW5pb24gQmFu
azEQMA4GA1UECxMHVERDTUItVjEPMA0GA1UEAxMGdGQuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAp3kVKAlyc1I+Ibjsdc2qAWSOiAamd0+coeKF
YOBFPVINrb3P1j6p0Ok04LZ3FAg0VOg/CZfUGOakaSUg7hTZtKEGB3txvYslFdxv
kX4bIVXvHzD9Sk2JTeyPV3JhAi4AOkqEuo4fbJyPVbvr88G1j5v9o9A3fIs5wBZq
cD0uWftgj5AsOoPIwfjHEe0sbg4BpZ092Ddq7v+61D8UccDjHCnkvx+czr5dU6VZ
/5YeNqLvOWxuaayuRY2zYUSCH7yDRHOY0pF0VxCyNG8fcECzbVa6AHgNC4t6K6ZC
yC745cqb0Ty/OQn+4Qbla4bnVzZe+CDUSl883ta28EwwrB6S1wIDAQABo4IDbTCC
A2kwHwYDVR0jBBgwFoAUPdNQpdagre7zSmAKZdMh1Pj41g8wHQYDVR0OBBYEFG4q
Vnq/yQW6Nkf5P4LhAujSnTkBMB0GA1UdEQQWMBSCBnRkLmNvbYIKd3d3LnRkLmNv
```

bTAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMC
MHUGA1UdHwRuMGwwNKAyoDCGLmh0dHA6Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9zaGEy
LWV2LXNlcnZlci1nMi5jcmwwNKAyoDCGLmh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNv
bS9zaGEyLWV2LXNlcnZlci1nMi5jcmwwSwYDVR0gBEQwQjA3BglghkgBhv1sAgEw
KjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cuZGlnaWNlcnQuY29tL0NQUzAHBgVn
gQwBATCBiAYIKwYBBQUHAQEEfDB6MCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC5k
aWdpY2VydC5jb20wUgYIKwYBBQUHMAKGRmh0dHA6Ly9jYWNlcnRzLmRpZ2ljZXJ0
LmNvbS9EaWdpQ2VydFNIQTJFeHRlbmRlZFZhbGlkYXRpb25TZXJ2ZXJDQS5jcnQw
CQYDVR0TBAIwADCCAX0GCisGAQQB1nkCBAIEggFtBIIBaQFnAHYApLkJkLQYWBSH
uxOizGdwCjw1mAT5G9+443fNDsgN3BAAAAFqvBr94QAABAMARzBFAiEA5T5sbwSJ
QPFsWyiI0eAy60Q/79Qz1cM/4U76T3xI1GICICV8PimVrCVQeIJxWBEglVKfAIRd
x7ME89sVudkG1GEFAHYAVhQGmi/XwuzT9eG9RLI+x0Z2ubyZEVzA75SYVdaJ0N0A
AAFqvBr6OwAABAMARzBFAiArX14Tb0JCym+tRjtG8AeCd1dhljNw1ujexVt2a+aV
hAIhAIJ+uU7JWpIJkUQse515uxZaYbjygHxZ4sxuCJH5XXNGAHUAh3W/51l8+IxD
mV+9827/Vo1HVjb/SrVgwbTq/16ggw8AAAFqvBr8AQAABAMARjBEAiA5F1TT7vUw
IkJYUkTjNUEpv/xlDjRcF7r7dSinaSS4GwIgYCrUoEjk/Efr9jQNido6M+tgz2FT
51EafPhDUAGUmJMwDQYJKoZIhvcNAQELBQADggEBACEfkKOMfaseMn8NkGfJGrbN
caFhk5bUYEgfpXecWOx/jX+b0AWfcqgeSNkxubV/erXJr8QqLmzfVb3U5jmBWRoL
9C+40MHjOyi0Le/IYYEFi+b+Xmv42GpROnij4VQ9HY3q3u1ln/Bq4EqmMTkrPZy0
JHNoyfWBypMQc/ymxQ3tgKEmb3QWAA5yvu3cgpMbKx49+7zd+NES8dxgyShvmlWA
ZGhWvl0VuC1Sa1oTVMj5KNHvl6MczBopTj3oBxpcAMYx91XmQS3AIuK3d4P3I344
qL8Mh8QdKxb6EhwhmXcR+zcuIMeGtVMwko55lqDykQi3uYCjgH7uPTPYB97GrgM=
-----END CERTIFICATE-----
1 s:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended Validation Server CA
i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert High Assurance EV Root CA
-----BEGIN CERTIFICATE-----
MIIEtjCCA56gAwIBAgIQDHmpRLCMEZUgkmFf4msdgzANBgkqhkiG9w0BAQsFADBs
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSswKQYDVQQDEyJEaWdpQ2VydCBIaWdoIEFzc3VyYW5j
ZSBFViBSb290IENBMB4XDTEzMTAyMjEyMDAwMFoXDTI4MTAyMjEyMDAwMFowdTEL
MAkGA1UEBhMCVVMxFTATBgNVBAoTDERpZ2lDZXJ0IEluYzEZMBcGA1UECxMQd3d3
LmRpZ2ljZXJ0LmNvbTE0MDIGA1UEAxMrRGlnaUNlcnQgU0hBMiBFeHRlbmRlZCBW
YWxpZGF0aW9uIFNlcnZlciBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBANdTpARR+JmmFkhLZyeqk0nQOe0MsLAAh/FnKIaFjI5j2ryxQDji0/XspQUY
uD0+xZkXMuwYjPrxDKZkIYXLBxA0sFKIKx9om9KxjxKws9LniB8f7zh3VFNfgHk/
LhqqqB5LKw2rt2O5Nbd9FLxZS99RStKh4gzikIKHaq7q12TWmFXo/a8aUGxUvBHy
/Urynbt/DvTVvo4WiRJV2MBxNO723C3sxIclho3YIeSwTQyJ3DkmF93215SF2AQh
cJ1vb/9cuhnhRctWVyh+HA1BV6q3uCe7seT6Ku8hI3UarS2bhjWMnHe1c63YlC3k
8wyd7sFOYn4XwHGeLN7x+RAoGTMCAwEAAaOCAUkwggFFMBIGA1UdEwEB/wQIMAYB
Af8CAQAwDgYDVR0PAQH/BAQDAgGGMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEF
BQcDAjA0BggrBgEFBQcBAQQoMCYwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmRp
Z2ljZXJ0LmNvbTBLBgNVHR8ERDBCMECgPqA8hjpodHRwOi8vY3JsNC5kaWdpY2Vy
dC5jb20vRGlnaUNlcnRIaWdoQXNzdXJhbmNlRVZSb290Q0EuY3JsMD0GA1UdIAQ2

MDQwMgYEVR0gADAqMCgGCCsGAQUFBwIBFhxodHRwczovL3d3dy5kaWdpY2VydC5j
b20vQ1BTMB0GA1UdDgQWBBQ901Cl1qCt7vNKYApl0yHU+PjWDzAfBgNVHSMEGDAW
gBSxPsNpA/i/RwHUmCYaCALvY2QrwzANBgkqhkiG9w0BAQsFAAOCAQEAnbbQkIbh
hgLtxaDwNBx0wY12zIYKqPBKikLWP8ipTa18CK3mtlC4ohpNiAexKSHc59rGPCHg
4xFJcKx6HQGkyhE6V6t9VypAdP3THYUYUN9XR3WhfVUgLkc3UHKMf4Ib0mKPLQNa
2sPIoc4sUqIAY+tzunHISScjl2SFnjgOrWNoPLpSgVh5oywM395t6zHyuqB8bPEs
1OG9d4Q3A84ytciagRpKkk47RpqF/oOi+Z6Mo8wNXrM9zwR4jxQUezKcxwCmXMS1
oVWNWlZopCJwqjyBcdmdqEU79OX2olHdx3ti6G8MdOu42vi/hw15UJGQmxg7kVkn
8TUoE6smftX3eg==
-----END CERTIFICATE-----
 2 s:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert High Assurance EV Root CA
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert High Assurance EV Root CA
-----BEGIN CERTIFICATE-----
MIIDxTCCAq2gAwIBAgIQAqxcJmoLQJuPC3nyrkYldzANBgkqhkiG9w0BAQUFADBs
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSswKQYDVQQDEyJEaWdpQ2VydCBIaWdoIEFzc3VyYW5j
ZSBFViBSb290IENBMB4XDTA2MTExMDAwMDAwMFoXDTMxMTExMDAwMDAwMFowbDEL
MAkGA1UEBhMCVVMxFTATBgNVBAoTDERpZ2lDZXJ0IEluYzEZMBcGA1UECxMQd3d3
LmRpZ2ljZXJ0LmNvbTErMCkGA1UEAxMiRGlnaUNlcnQgSGlnaCBBc3N1cmFuY2Ug
RVYgUm9vdCBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMbM5XPm
+9S75S0tMqbf5YE/yc0lSbZxKsPVlDRnogocsF9ppkCxxLeyj9CYpKlBWTrT3JTW
PNt0OKRKzE0lgvdKpVMSOO7zSW1xkX5jtqumX8OkhPhPYlG++MXs2ziS4wblCJEM
xChBVfvLWokVfnHoNb9Ncgk9vjo4UFt3MRuNs8ckRZqnrG0AFFoEt7oT61EKmEFB
Ik5lYYeBQVCmeVyJ3hlKV9Uu5l0cUyx+mM0aBhakaHPQNAQTXKFx01p8VdteZOE3
hzBWBOURtCmAEvF5OYiiAhF8J2a3iLd48soKqDirCmTCv2ZdlYTBoSUeh10aUAsg
EsxBu24LUTi4S8sCAwEAAaNjMGEwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQF
MAMBAf8wHQYDVR0OBBYEFLE+w2kD+L9HAdSYJhoIAu9jZCvDMB8GA1UdIwQYMBaA
FLE+w2kD+L9HAdSYJhoIAu9jZCvDMA0GCSqGSIb3DQEBBQUAA4IBAQAcGgaX3Nec
nzyIZgYIVyHbIUf4KmeqvxgydkAQV8GK83rZEWWONfqe/EW1ntlMMUu4kehDLI6z
eM7b41N5cdblIZQB2lWHmiRk9opmzN6cN82oNLFpmyPInngiK3BD41VHMWEZ71jF
hS9OMPagMRYjyOfiZRYzy78aG6A9+MpeizGLYAiJLQwGXFK3xPkKmNEVX58Svnw2
Yzi9RKR/5CYrCsSXaQ3pjOLAEFe4yHYSkVXySGnYvCoCWw9E1CAx2/S6cCZdkGCe
vEsXCS+0yx5DaMkHJ8HSXPfqIblоEpw8nL+e/IBcm2PN7EeqJSdnoDfzAIJ9VNep
+OkuE6N36B9K
-----END CERTIFICATE-----

Server certificate
subject=/businessCategory=Private Organization/jurisdictionC=CA/jurisdictionST=Nova Scotia/serialNumber=1010197/C=CA/ST=Ontario/L=Toronto/O=The Toronto-Dominion Bank/OU=TDCMB-V/CN=td.com
issuer=/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended Validation Server CA

No client certificate CA names sent

Peer signing digest: SHA256
Server Temp Key: ECDH, P-256, 256 bits

SSL handshake has read 4710 bytes and written 431 bytes

New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
  Protocol : TLSv1.2
  Cipher   : ECDHE-RSA-AES128-GCM-SHA256
  Session-ID: C36EC96DBCC3BACA20901BB0938A8B3E014ECFE618A7786B947F7484ADBED178
  Session-ID-ctx:
  Master-Key:
9429B906AF23B712864A0F9456BBBF47DD6B24440E4E40EE0FB7A7B087AA3EB1A9E5B08A860
81488DE1A202E8F9A0591
  Key-Arg   : None
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  TLS session ticket lifetime hint: 7200 (seconds)
  TLS session ticket:
  0000 - f1 c0 93 03 cc 68 1b b1-28 90 33 90 ff 03 51 b6   .....h..(.3...Q.
  0010 - e3 05 30 39 6c 4f a4 94-68 3b fc ca 00 a8 7c aa   ..09lO..h;....|.
  0020 - d4 be 23 34 f9 d3 51 6b-f7 45 94 d9 4b 82 ff ce   ..#4..Qk.E..K...
  0030 - 9f 09 79 01 3f dc 9d 6b-82 71 d2 ce 4c 50 5b bf   ..y.?..k.q..LP[.
  0040 - 7b 4c 37 1b ff 9d cd 50-c9 b2 70 a0 dd 63 0f 5a   {L7....P..p..c.Z
  0050 - 75 6a f8 36 11 43 a0 14-09 4e 0f a9 19 e4 db 7a   uj.6.C...N.....z
  0060 - 88 db a0 fd e0 ae 18 9a-ef e1 6d d8 ee b2 ee ab   ....m.....
  0070 - 14 8e 33 42 db 50 f3 89-42 ff 40 20 38 5d 25 50   ..3B.P..B.@ 8]%P
  0080 - 00 ef 02 8c c8 bf 51 ad-d3 1b 9a 0e d1 fd 1e 5b   ......Q........[
  0090 - 69 6f bb f1 6b 31 51 e4-9a d1 22 4a 04 89 15 df   io..k1Q..."J....

  Start Time: 1603175420
  Timeout   : 300 (sec)
  Verify return code: 0 (ok)

********** **c0.pem** **********

-----BEGIN CERTIFICATE-----
MIIHSzCCBjOgAwIBAgIQB9gt165ngvgCSAaF425BXzANBgkqhkiG9w0BAQsFADB1

```
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMTQwMgYDVQQDEytEaWdpQ2VydCBTSEEyIEV4dGVuZGVk
IFZhbGlkYXRpb24gU2VydmVyIENBMB4XDTE5MDUxNTAwMDAwMFoXDTIxMDExMTEy
MDAwMFowgdwxHTAbBgNVBA8MFFByaXZhdGUgT3JnYW5pemF0aW9uMRMwEQYLKwYB
BAGCNzwCAQMTAkNBMRwwGgYLKwYBBAGCNzwCAQITC05vdmEgU2NvdGlhMRAwDgYD
VQQFEwcxMDEwMTk3MQswCQYDVQQGEwJDQTEQMA4GA1UECBMHT250YXJpbzEQMA4G
A1UEBxMHVG9yb250bzEiMCAGA1UEChMZVGhlIFRvcm9udG8tRG9taW5pb24gQmFu
azEQMA4GA1UECxMHVERDTUItVjEPMA0GA1UEAxMGdGQuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAp3kVKAlyc1I+Ibjsdc2qAWSOiAamd0+coeKF
YOBFPVINrb3P1j6p0Ok04LZ3FAg0VOg/CZfUGOakaSUg7hTZtKEGB3txvYslFdxv
kX4bIVXvHzD9Sk2JTeyPV3JhAi4AOkqEuo4fbJyPVbvr88G1j5v9o9A3fIs5wBZq
cD0uWftgj5AsOoPIwfjHEe0sbg4BpZ092Ddq7v+61D8UccDjHCnkvx+czr5dU6VZ
/5YeNqLvOWxuaayuRY2zYUSCH7yDRHOY0pF0VxCyNG8fcECzbVa6AHgNC4t6K6ZC
yC745cqb0Ty/OQn+4Qbla4bnVzZe+CDUSl883ta28EwwrB6S1wIDAQABo4IDbTCC
A2kwHwYDVR0jBBgwFoAUPdNQpdagre7zSmAKZdMh1Pj41g8wHQYDVR0OBBYEFG4q
Vnq/yQW6Nkf5P4LhAujSnTkBMB0GA1UdEQQWMBSCBnRkLmNvbYIKd3d3LnRkLmNv
bTAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMC
MHUGA1UdHwRuMGwwNKAyoDCGLmh0dHA6Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9zaGEy
LWV2LXNlcnZlci1nMi5jcmwwNKAyoDCGLmh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNv
bS9zaGEyLWV2LXNlcnZlci1nMi5jcmwwSwYDVR0gBEQwQjA3BglghkgBhv1sAgEw
KjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cuZGlnaWNlcnQuY29tL0NQUzAHBgVn
gQwBATCBiAYIKwYBBQUHAQEEfDB6MCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC5k
aWdpY2VydC5jb20wUgYIKwYBBQUHMAKGRmh0dHA6Ly9jYWNlcnRzLmRpZ2ljZXJ0
LmNvbS9EaWdpQ2VydFNIQTJFeHRlbmRlZFZhbGlkYXRpb25TZXJ2ZXJDQS5jcnQw
CQYDVR0TBAIwADCCAX0GCisGAQQB1nkCBAIEggFtBIIBaQFnAHYApLkJkLQYWBSH
uxOizGdwCjw1mAT5G9+443fNDsgN3BAAAAFqvBr94QAABAMARzBFAiEA5T5sbwSJ
QPFsWyiI0eAy60Q/79Qz1cM/4U76T3xI1GICICV8PimVrCVQeIJxWBEglVKfAIRd
x7ME89sVudkG1GEFAHYAVhQGmi/XwuzT9eG9RLI+x0Z2ubyZEVzA75SYVdaJ0N0A
AAFqvBr6OwAABAMARzBFAiArX14Tb0JCym+tRjtG8AeCd1dhljNw1ujexVt2a+aV
hAIhAIJ+uU7JWpIJkUQse515uxZaYbjygHxZ4sxuCJH5XXNGAHUAh3W/51l8+IxD
mV+9827/Vo1HVjb/SrVgwbTq/16ggw8AAAFqvBr8AQAABAMARjBEAiA5F1TT7vUw
IkJYUkTjNUEpv/xlDjRcF7r7dSinaSS4GwIgYCrUoEjk/Efr9jQNido6M+tgz2FT
51EafPhDUAGUmJMwDQYJKoZIhvcNAQELBQADggEBACEfkKOMfaseMn8NkGfJGrbN
caFhk5bUYEgfpXecWOx/jX+b0AWfcqgeSNkxubV/erXJr8QqLmzfVb3U5jmBWRoL
9C+40MHjOyi0Le/IYYEFi+b+Xmv42GpROnij4VQ9HY3q3u1ln/Bq4EqmMTkrPZy0
JHNoyfWBypMQc/ymxQ3tgKEmb3QWAA5yvu3cgpMbKx49+7zd+NES8dxgyShvmlWA
ZGhWvl0VuC1Sa1oTVMj5KNHvl6MczBopTj3oBxpcAMYx91XmQS3AIuK3d4P3I344
qL8Mh8QdKxb6EhwhmXcR+zcuIMeGtVMwko55lqDykQi3uYCjgH7uPTPYB97GrgM=
-----END CERTIFICATE-----
```

******************************** c1.pem ************************************

```
-----BEGIN CERTIFICATE-----
MIIEtjCCA56gAwIBAgIQDHmpRLCMEZUgkmFf4msdgzANBgkqhkiG9w0BAQsFADBs
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSswKQYDVQQDEyJEaWdpQ2VydCBIaWdoIEFzc3VyYW5j
ZSBFViBSb290IENBMB4XDTEzMTAyMjEyMDAwMFoXDTI4MTAyMjEyMDAwMFowdTEL
MAkGA1UEBhMCVVMxFTATBgNVBAoTDERpZ2lDZXJ0IEluYzEZMBcGA1UECxMQd3d3
LmRpZ2ljZXJ0LmNvbTE0MDIGA1UEAxMrRGlnaUNlcnQgU0hBMiBFeHRlbmRlZCBW
YWxpZGF0aW9uIFNlcnZlciBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBANdTpARR+JmmFkhLZyeqk0nQOe0MsLAAh/FnKIaFjI5j2ryxQDji0/XspQUY
uD0+xZkXMuwYjPrxDKZkIYXLBxA0sFKIKx9om9KxjxKws9LniB8f7zh3VFNfgHk/
LhqqqB5LKw2rt2O5Nbd9FLxZS99RStKh4gzikIKHaq7q12TWmFXo/a8aUGxUvBHy
/Urynbt/DvTVvo4WiRJV2MBxNO723C3sxIclho3YIeSwTQyJ3DkmF93215SF2AQh
cJ1vb/9cuhnhRctWVyh+HA1BV6q3uCe7seT6Ku8hI3UarS2bhjWMnHe1c63YlC3k
```

```
8wyd7sFOYn4XwHGeLN7x+RAoGTMCAwEAAaOCAUkwggFFMBIGA1UdEwEB/wQIMAYB
Af8CAQAwDgYDVR0PAQH/BAQDAgGGMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEF
BQcDAjA0BggrBgEFBQcBAQQoMCYwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmRp
Z2ljZXJ0LmNvbTBLBgNVHR8ERDBCMECgPqA8hjpodHRwOi8vY3JsNC5kaWdpY2Vy
dC5jb20vRGlnaUNlcnRIaWdoQXNzdXJhbmNlRVZSb290Q0EuY3JsMD0GA1UdIAQ2
MDQwMgYEVR0gADAqMCgGCCsGAQUFBwIBFhxodHRwczovL3d3dy5kaWdpY2VydC5j
b20vQ1BTMB0GA1UdDgQWBBQ901Cl1qCt7vNKYApl0yHU+PjWDzAfBgNVHSMEGDAW
gBSxPsNpA/i/RwHUmCYaCALvY2QrwzANBgkqhkiG9w0BAQsFAAOCAQEAnbbQkIbh
hgLtxaDwNBx0wY12zIYKqPBKikLWP8ipTa18CK3mtlC4ohpNiAexKSHc59rGPCHg
4xFJcKx6HQGkyhE6V6t9VypAdP3THYUYUN9XR3WhfVUgLkc3UHKMf4Ib0mKPLQNa
2sPIoc4sUqIAY+tzunHISScjl2SFnjgOrWNoPLpSgVh5oywM395t6zHyuqB8bPEs
1OG9d4Q3A84ytciagRpKkk47RpqF/oOi+Z6Mo8wNXrM9zwR4jxQUezKcxwCmXMS1
oVWNWlZopCJwqjyBcdmdqEU79OX2olHdx3ti6G8MdOu42vi/hw15UJGQmxg7kVkn
8TUoE6smftX3eg==
-----END CERTIFICATE-----
```

2. ********** **Command** **********

```
[10/20/20]seed@VM:~$  openssl x509 -in c1.pem -noout -modulus
Modulus=D753A40451F899A616484B6727AA9349D039ED0CB0B00087F1672886858C8E63DAB
CB14038E2D3F5ECA50518B83D3EC5991732EC188CFAF10CA6642185CB071034B052882B1F689
BD2B18F12B0B3D2E7881F1FEF387754535F80793F2E1AAAA81E4B2B0DABB763B935B77D14BC
594BDF514AD2A1E20CE29082876AAEEAD764D69855E8FDAF1A506C54BC11F2FD4AF29DBB7F0
EF4D5BE8E16891255D8C07134EEF6DC2DECC48725868DD821E4B04D0C89DC392617DDF6D794
85D80421709D6F6FFF5CBA19E145CB5657287E1C0D4157AAB7B827BBB1E4FA2AEF2123751AA
D2D9B86358C9C77B573ADD8942DE4F30C9DEEC14E627E17C0719E2CDEF1F910281933

[10/20/20]seed@VM:~$ openssl x509 -in c1.pem -text -noout
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      0c:79:a9:44:b0:8c:11:95:20:92:61:5f:e2:6b:1d:83
  Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert High Assurance EV Root
CA
    Validity
      Not Before: Oct 22 12:00:00 2013 GMT
      Not After : Oct 22 12:00:00 2028 GMT
    Subject: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended
Validation Server CA
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
          00:d7:53:a4:04:51:f8:99:a6:16:48:4b:67:27:aa:
          93:49:d0:39:ed:0c:b0:b0:00:87:f1:67:28:86:85:
          8c:8e:63:da:bc:b1:40:38:e2:d3:f5:ec:a5:05:18:
```

```
            b8:3d:3e:c5:99:17:32:ec:18:8c:fa:f1:0c:a6:64:
            21:85:cb:07:10:34:b0:52:88:2b:1f:68:9b:d2:b1:
            8f:12:b0:b3:d2:e7:88:1f:1f:ef:38:77:54:53:5f:
            80:79:3f:2e:1a:aa:a8:1e:4b:2b:0d:ab:b7:63:b9:
            35:b7:7d:14:bc:59:4b:df:51:4a:d2:a1:e2:0c:e2:
            90:82:87:6a:ae:ea:d7:64:d6:98:55:e8:fd:af:1a:
            50:6c:54:bc:11:f2:fd:4a:f2:9d:bb:7f:0e:f4:d5:
            be:8e:16:89:12:55:d8:c0:71:34:ee:f6:dc:2d:ec:
            c4:87:25:86:8d:d8:21:e4:b0:4d:0c:89:dc:39:26:
            17:dd:f6:d7:94:85:d8:04:21:70:9d:6f:6f:ff:5c:
            ba:19:e1:45:cb:56:57:28:7e:1c:0d:41:57:aa:b7:
            b8:27:bb:b1:e4:fa:2a:ef:21:23:75:1a:ad:2d:9b:
            86:35:8c:9c:77:b5:73:ad:d8:94:2d:e4:f3:0c:9d:
            ee:c1:4e:62:7e:17:c0:71:9e:2c:de:f1:f9:10:28:
            19:33
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints: critical
        CA:TRUE, pathlen:0
      X509v3 Key Usage: critical
        Digital Signature, Certificate Sign, CRL Sign
      X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client Authentication
      Authority Information Access:
        OCSP - URI:http://ocsp.digicert.com

      X509v3 CRL Distribution Points:

        Full Name:
          URI:http://crl4.digicert.com/DigiCertHighAssuranceEVRootCA.crl

      X509v3 Certificate Policies:
        Policy: X509v3 Any Policy
          CPS: https://www.digicert.com/CPS

      X509v3 Subject Key Identifier:
        3D:D3:50:A5:D6:A0:AD:EE:F3:4A:60:0A:65:D3:21:D4:F8:F8:D6:0F
      X509v3 Authority Key Identifier:
        keyid:B1:3E:C3:69:03:F8:BF:47:01:D4:98:26:1A:08:02:EF:63:64:2B:C3

  Signature Algorithm: sha256WithRSAEncryption
     9d:b6:d0:90:86:e1:86:02:ed:c5:a0:f0:34:1c:74:c1:8d:76:
     cc:86:0a:a8:f0:4a:8a:42:d6:3f:c8:a9:4d:ad:7c:08:ad:e6:
     b6:50:b8:a2:1a:4d:88:07:b1:29:21:dc:e7:da:c6:3c:21:e0:
```

e3:11:49:70:ac:7a:1d:01:a4:ca:11:3a:57:ab:7d:57:2a:40:
74:fd:d3:1d:85:18:50:df:57:47:75:a1:7d:55:20:2e:47:37:
50:72:8c:7f:82:1b:d2:62:8f:2d:03:5a:da:c3:c8:a1:ce:2c:
52:a2:00:63:eb:73:ba:71:c8:49:27:23:97:64:85:9e:38:0e:
ad:63:68:3c:ba:52:81:58:79:a3:2c:0c:df:de:6d:eb:31:f2:
ba:a0:7c:6c:f1:2c:d4:e1:bd:77:84:37:03:ce:32:b5:c8:9a:
81:1a:4a:92:4e:3b:46:9a:85:fe:83:a2:f9:9e:8c:a3:cc:0d:
5e:b3:3d:cf:04:78:8f:14:14:7b:32:9c:c7:00:a6:5c:c4:b5:
a1:55:8d:5a:56:68:a4:22:70:aa:3c:81:71:d9:9d:a8:45:3b:
f4:e5:f6:a2:51:dd:c7:7b:62:e8:6f:0c:74:eb:b8:da:f8:bf:
87:0d:79:50:91:90:9b:18:3b:91:59:27:f1:35:28:13:ab:26:
7e:d5:f7:7a

3. ********** **Command** **********

[10/20/20]seed@VM:~$ openssl x509 -in c0.pem -text -noout
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      07:d8:2d:d7:ae:67:82:f8:02:48:06:85:e3:6e:41:5f
  Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA
    Validity
      Not Before: May 15 00:00:00 2019 GMT
      Not After : Jan 11 12:00:00 2021 GMT
    Subject: businessCategory=Private Organization/jurisdictionC=CA/jurisdictionST=Nova Scotia/serialNumber=1010197, C=CA, ST=Ontario, L=Toronto, O=The Toronto-Dominion Bank, OU=TDCMB-V, CN=td.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
          00:a7:79:15:28:09:72:73:52:3e:21:b8:ec:75:cd:
          aa:01:64:8e:88:06:a6:77:4f:9c:a1:e2:85:60:e0:
          45:3d:52:0d:ad:bd:cf:d6:3e:a9:d0:e9:34:e0:b6:
          77:14:08:34:54:e8:3f:09:97:d4:18:e6:a4:69:25:
          20:ee:14:d9:b4:a1:06:07:7b:71:bd:8b:25:15:dc:
          6f:91:7e:1b:21:55:ef:1f:30:fd:4a:4d:89:4d:ec:
          8f:57:72:61:02:2e:00:3a:4a:84:ba:8e:1f:6c:9c:
          8f:55:bb:eb:f3:c1:b5:8f:9b:fd:a3:d0:37:7c:8b:
          39:c0:16:6a:70:3d:2e:59:fb:60:8f:90:2c:3a:83:
          c8:c1:f8:c7:11:ed:2c:6e:0e:01:a5:9d:3d:d8:37:
          6a:ee:ff:ba:d4:3f:14:71:c0:e3:1c:29:e4:bf:1f:

```
                9c:ce:be:5d:53:a5:59:ff:96:1e:36:a2:ef:39:6c:
                6e:69:ac:ae:45:8d:b3:61:44:82:1f:bc:83:44:73:
                98:d2:91:74:57:10:b2:34:6f:1f:70:40:b3:6d:56:
                ba:00:78:0d:0b:8b:7a:2b:a6:42:c8:2e:f8:e5:ca:
                9b:d1:3c:bf:39:09:fe:e1:06:e5:6b:86:e7:57:36:
                5e:f8:20:d4:4a:5f:3c:de:d6:b6:f0:4c:30:ac:1e:
                92:d7
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:3D:D3:50:A5:D6:A0:AD:EE:F3:4A:60:0A:65:D3:21:D4:F8:F8:D6:0F

            X509v3 Subject Key Identifier:
                6E:2A:56:7A:BF:C9:05:BA:36:47:F9:3F:82:E1:02:E8:D2:9D:39:01
            X509v3 Subject Alternative Name:
                DNS:td.com, DNS:www.td.com
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://crl3.digicert.com/sha2-ev-server-g2.crl

                Full Name:
                  URI:http://crl4.digicert.com/sha2-ev-server-g2.crl

            X509v3 Certificate Policies:
                Policy: 2.16.840.1.114412.2.1
                  CPS: https://www.digicert.com/CPS
                Policy: 2.23.140.1.1

            Authority Information Access:
                OCSP - URI:http://ocsp.digicert.com
                CA Issuers -
URI:http://cacerts.digicert.com/DigiCertSHA2ExtendedValidationServerCA.crt

            X509v3 Basic Constraints:
                CA:FALSE
            CT Precertificate SCTs:
                Signed Certificate Timestamp:
                    Version   : v1(0)
                    Log ID    : A4:B9:09:90:B4:18:58:14:87:BB:13:A2:CC:67:70:0A:
```

```
            3C:35:98:04:F9:1B:DF:B8:E3:77:CD:0E:C8:0D:DC:10
        Timestamp : May 15 15:27:26.689 2019 GMT
        Extensions: none
        Signature : ecdsa-with-SHA256
            30:45:02:21:00:E5:3E:6C:6F:04:89:40:F1:6C:5B:28:
            88:D1:E0:32:EB:44:3F:EF:D4:33:D5:C3:3F:E1:4E:FA:
            4F:7C:48:D4:62:02:20:25:7C:3E:29:95:AC:25:50:78:
            82:71:58:11:20:95:52:9F:00:84:5D:C7:B3:04:F3:DB:
            15:B9:D9:06:D4:61:05
    Signed Certificate Timestamp:
        Version   : v1(0)
        Log ID    : 56:14:06:9A:2F:D7:C2:EC:D3:F5:E1:BD:44:B2:3E:C7:
            46:76:B9:BC:99:11:5C:C0:EF:94:98:55:D6:89:D0:DD
        Timestamp : May 15 15:27:25.755 2019 GMT
        Extensions: none
        Signature : ecdsa-with-SHA256
            30:45:02:20:2B:5F:5E:13:6F:42:42:CA:6F:AD:46:3B:
            46:F0:07:82:77:57:61:96:33:70:D6:E8:DE:C5:5B:76:
            6B:E6:95:84:02:21:00:82:7E:B9:4E:C9:5A:92:09:91:
            44:2C:7B:9D:79:BB:16:5A:61:B8:F2:80:7C:59:E2:CC:
            6E:08:91:F9:5D:73:46
    Signed Certificate Timestamp:
        Version   : v1(0)
        Log ID    : 87:75:BF:E7:59:7C:F8:8C:43:99:5F:BD:F3:6E:FF:56:
            8D:47:56:36:FF:4A:B5:60:C1:B4:EA:FF:5E:A0:83:0F
        Timestamp : May 15 15:27:26.209 2019 GMT
        Extensions: none
        Signature : ecdsa-with-SHA256
            30:44:02:20:39:17:54:D3:EE:F5:30:22:42:58:52:44:
            E3:35:41:29:BF:FC:65:0E:34:5C:17:BA:FB:75:28:A7:
            69:24:B8:1B:02:20:60:2A:D4:A0:48:E4:FC:47:EB:F6:
            34:0D:89:DA:3A:33:EB:60:CF:61:53:E7:51:1A:7C:F8:
            43:50:01:94:98:93
Signature Algorithm: sha256WithRSAEncryption
    21:1f:90:a3:8c:7d:ab:1e:32:7f:0d:90:67:c9:1a:b6:cd:71:
    a1:61:93:96:d4:60:48:1f:a5:77:9c:58:ec:7f:8d:7f:9b:d0:
    05:9f:72:a8:1e:48:d9:31:b9:b5:7f:7a:b5:c9:af:c4:2a:2e:
    6c:df:55:bd:d4:e6:39:81:59:1a:0b:f4:2f:b8:d0:c1:e3:3b:
    28:b4:2d:ef:c8:61:81:05:8b:e6:fe:5e:6b:f8:d8:6a:51:3a:
    78:a3:e1:54:3d:1d:8d:ea:de:ed:65:9f:f0:6a:e0:4a:a6:31:
    39:2b:3d:9c:b4:24:73:68:c9:f5:81:ca:93:10:73:fc:a6:c5:
    0d:ed:80:a1:26:6f:74:16:00:0e:72:be:ed:dc:82:93:1b:2b:
    1e:3d:fb:bc:dd:f8:d1:12:f1:dc:60:c9:28:6f:9a:55:80:64:
    68:56:be:5d:15:b8:2d:52:6b:5a:13:54:c8:f9:28:d1:ef:97:
```

a3:1c:cc:1a:29:4e:3d:e8:07:1a:5c:00:c6:31:f7:55:e6:41:
2d:c0:22:e2:b7:77:83:f7:23:7e:38:a8:bf:0c:87:c4:1d:2b:
16:fa:12:1c:21:99:77:11:fb:37:2e:20:c7:86:b5:53:30:92:
8e:79:96:a0:f2:91:08:b7:b9:80:a3:80:7e:ee:3d:33:d8:07:
de:c6:ae:03

[10/20/20]seed@VM:~$ cat temp.txt | tr -d â€™[:space:]:â€™
211f90a38c7dab1e327f0d9067c91ab6cd71a1619396d460481fa5779c58ec7f8d7f9bd0059f72a8
1e48d931b9b57f7ab5c9afc42a2e6cdf55bdd4e63981591a0bf42fb8d0c1e33b28b42defc8618105
8be6fe5e6bf8d86a513a78a3e1543d1d8deadeed659ff06ae04aa631392b3d9cb4247368c9f581ca
931073fca6c50ded80a1266f7416000e72beeddc82931b2b1e3dfbbcddf8d112f1dc60c9286f9a55
80646856be5d15b82d526b5a1354c8f928d1ef97a31ccc1a294e3de8071a5c00c631f755e6412dc
022e2b77783f7237e38a8bf0c87c41d2b16fa121c21997711fb372e20c786b55330928e7996a0f29
108b7b980a3807eee3d33d807dec6ae03

4. ********** **Command** **********

[10/20/20]seed@VM:~$ openssl asn1parse -i -in c0.pem
```
    0:d=0  hl=4 l=1867 cons: SEQUENCE
    4:d=1  hl=4 l=1587 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=  16 prim:   INTEGER           :07D82DD7AE6782F802480685E36E415F
   31:d=2  hl=2 l=  13 cons:   SEQUENCE
   33:d=3  hl=2 l=   9 prim:    OBJECT            :sha256WithRSAEncryption
   44:d=3  hl=2 l=   0 prim:    NULL
   46:d=2  hl=2 l= 117 cons:   SEQUENCE
   48:d=3  hl=2 l=  11 cons:    SET
   50:d=4  hl=2 l=   9 cons:     SEQUENCE
   52:d=5  hl=2 l=   3 prim:      OBJECT            :countryName
   57:d=5  hl=2 l=   2 prim:      PRINTABLESTRING   :US
   61:d=3  hl=2 l=  21 cons:    SET
   63:d=4  hl=2 l=  19 cons:     SEQUENCE
   65:d=5  hl=2 l=   3 prim:      OBJECT            :organizationName
   70:d=5  hl=2 l=  12 prim:      PRINTABLESTRING   :DigiCert Inc
   84:d=3  hl=2 l=  25 cons:    SET
   86:d=4  hl=2 l=  23 cons:     SEQUENCE
   88:d=5  hl=2 l=   3 prim:      OBJECT            :organizationalUnitName
   93:d=5  hl=2 l=  16 prim:      PRINTABLESTRING   :www.digicert.com
  111:d=3  hl=2 l=  52 cons:    SET
  113:d=4  hl=2 l=  50 cons:     SEQUENCE
  115:d=5  hl=2 l=   3 prim:      OBJECT            :commonName
  120:d=5  hl=2 l=  43 prim:      PRINTABLESTRING   :DigiCert SHA2 Extended Validation Server CA
```

```
165:d=2  hl=2 l=  30 cons:  SEQUENCE
167:d=3  hl=2 l=  13 prim:   UTCTIME         :190515000000Z
182:d=3  hl=2 l=  13 prim:   UTCTIME         :210111120000Z
197:d=2  hl=3 l= 220 cons:  SEQUENCE
200:d=3  hl=2 l=  29 cons:   SET
202:d=4  hl=2 l=  27 cons:    SEQUENCE
204:d=5  hl=2 l=   3 prim:     OBJECT          :businessCategory
209:d=5  hl=2 l=  20 prim:     UTF8STRING      :Private Organization
231:d=3  hl=2 l=  19 cons:   SET
233:d=4  hl=2 l=  17 cons:    SEQUENCE
235:d=5  hl=2 l=  11 prim:     OBJECT          :jurisdictionCountryName
248:d=5  hl=2 l=   2 prim:     PRINTABLESTRING   :CA
252:d=3  hl=2 l=  28 cons:   SET
254:d=4  hl=2 l=  26 cons:    SEQUENCE
256:d=5  hl=2 l=  11 prim:     OBJECT          :jurisdictionStateOrProvinceName
269:d=5  hl=2 l=  11 prim:     PRINTABLESTRING   :Nova Scotia
282:d=3  hl=2 l=  16 cons:   SET
284:d=4  hl=2 l=  14 cons:    SEQUENCE
286:d=5  hl=2 l=   3 prim:     OBJECT          :serialNumber
291:d=5  hl=2 l=   7 prim:     PRINTABLESTRING   :1010197
300:d=3  hl=2 l=  11 cons:   SET
302:d=4  hl=2 l=   9 cons:    SEQUENCE
304:d=5  hl=2 l=   3 prim:     OBJECT          :countryName
309:d=5  hl=2 l=   2 prim:     PRINTABLESTRING   :CA
313:d=3  hl=2 l=  16 cons:   SET
315:d=4  hl=2 l=  14 cons:    SEQUENCE
317:d=5  hl=2 l=   3 prim:     OBJECT          :stateOrProvinceName
322:d=5  hl=2 l=   7 prim:     PRINTABLESTRING   :Ontario
331:d=3  hl=2 l=  16 cons:   SET
333:d=4  hl=2 l=  14 cons:    SEQUENCE
335:d=5  hl=2 l=   3 prim:     OBJECT          :localityName
340:d=5  hl=2 l=   7 prim:     PRINTABLESTRING   :Toronto
349:d=3  hl=2 l=  34 cons:   SET
351:d=4  hl=2 l=  32 cons:    SEQUENCE
353:d=5  hl=2 l=   3 prim:     OBJECT          :organizationName
358:d=5  hl=2 l=  25 prim:     PRINTABLESTRING   :The Toronto-Dominion Bank
385:d=3  hl=2 l=  16 cons:   SET
387:d=4  hl=2 l=  14 cons:    SEQUENCE
389:d=5  hl=2 l=   3 prim:     OBJECT          :organizationalUnitName
394:d=5  hl=2 l=   7 prim:     PRINTABLESTRING   :TDCMB-V
403:d=3  hl=2 l=  15 cons:   SET
405:d=4  hl=2 l=  13 cons:    SEQUENCE
407:d=5  hl=2 l=   3 prim:     OBJECT          :commonName
412:d=5  hl=2 l=   6 prim:     PRINTABLESTRING   :td.com
```

```
  420:d=2  hl=4 l= 290 cons:   SEQUENCE
  424:d=3  hl=2 l=  13 cons:    SEQUENCE
  426:d=4  hl=2 l=   9 prim:     OBJECT           :rsaEncryption
  437:d=4  hl=2 l=   0 prim:     NULL
  439:d=3  hl=4 l= 271 prim:    BIT STRING
  714:d=2  hl=4 l= 877 cons:   cont [ 3 ]
  718:d=3  hl=4 l= 873 cons:    SEQUENCE
  722:d=4  hl=2 l=  31 cons:     SEQUENCE
  724:d=5  hl=2 l=   3 prim:      OBJECT           :X509v3 Authority Key Identifier
  729:d=5  hl=2 l=  24 prim:      OCTET STRING      [HEX
DUMP]:301680143DD350A5D6A0ADEEF34A600A65D321D4F8F8D60F
  755:d=4  hl=2 l=  29 cons:     SEQUENCE
  757:d=5  hl=2 l=   3 prim:      OBJECT           :X509v3 Subject Key Identifier
  762:d=5  hl=2 l=  22 prim:      OCTET STRING      [HEX
DUMP]:04146E2A567ABFC905BA3647F93F82E102E8D29D3901
  786:d=4  hl=2 l=  29 cons:     SEQUENCE
  788:d=5  hl=2 l=   3 prim:      OBJECT           :X509v3 Subject Alternative Name
  793:d=5  hl=2 l=  22 prim:      OCTET STRING      [HEX
DUMP]:3014820674642E636F6D820A7777772E74642E636F6D
  817:d=4  hl=2 l=  14 cons:     SEQUENCE
  819:d=5  hl=2 l=   3 prim:      OBJECT           :X509v3 Key Usage
  824:d=5  hl=2 l=   1 prim:      BOOLEAN          :255
  827:d=5  hl=2 l=   4 prim:      OCTET STRING      [HEX DUMP]:030205A0
  833:d=4  hl=2 l=  29 cons:     SEQUENCE
  835:d=5  hl=2 l=   3 prim:      OBJECT           :X509v3 Extended Key Usage
  840:d=5  hl=2 l=  22 prim:      OCTET STRING      [HEX
DUMP]:301406082B06010505070301060 82B06010505070302
  864:d=4  hl=2 l= 117 cons:     SEQUENCE
  866:d=5  hl=2 l=   3 prim:      OBJECT           :X509v3 CRL Distribution Points
  871:d=5  hl=2 l= 110 prim:      OCTET STRING      [HEX
DUMP]:306C3034A032A030862E687474703A2F2F63726C332E64696769636572742E636F6D2F
736861322D65762D7365727665722D67322E63726C3034A032A030862E687474703A2F2F6372
6C342E64696769636572742E636F6D2F736861322D65762D7365727665722D67322E63726C
  983:d=4  hl=2 l=  75 cons:     SEQUENCE
  985:d=5  hl=2 l=   3 prim:      OBJECT           :X509v3 Certificate Policies
  990:d=5  hl=2 l=  68 prim:      OCTET STRING      [HEX
DUMP]:3042303706096086480186FD6C0201302A302806082B06010505070201161C68747470
733A2F2F7777772E64696769636572742E636F6D2F435053300706056781 0C0101
 1060:d=4  hl=3 l= 136 cons:     SEQUENCE
 1063:d=5  hl=2 l=   8 prim:      OBJECT           :Authority Information Access
 1073:d=5  hl=2 l= 124 prim:      OCTET STRING      [HEX
DUMP]:307A302406082B06010505073001861 8687474703A2F2F6F6373702E646967696365727
42E636F6D305206082B06010505073002864 6687474703A2F2F636163657274732E6469676963
```

6572742E636F6D2F446967694365727453484132457874656E64656456616C69646174696F6E5
3657276657243412E637274
1199:d=4 hl=2 l= 9 cons: SEQUENCE
1201:d=5 hl=2 l= 3 prim: OBJECT :X509v3 Basic Constraints
1206:d=5 hl=2 l= 2 prim: OCTET STRING [HEX DUMP]:3000
1210:d=4 hl=4 l= 381 cons: SEQUENCE
1214:d=5 hl=2 l= 10 prim: OBJECT :CT Precertificate SCTs
1226:d=5 hl=4 l= 365 prim: OCTET STRING [HEX
DUMP]:048201690167007600A4B90990B418581487BB13A2CC67700A3C359804F91BDFB8E377
CD0EC80DDC100000016ABC1AFDE10000040300473045022100E53E6C6F048940F16C5B2888D1
E032EB443FEFD433D5C33FE14EFA4F7C48D4620220257C3E2995AC25507882715811209552 9F0
0845DC7B304F3DB15B9D906D461050076005614069A2FD7C2ECD3F5E1BD44B23EC74676B9BC
99115CC0EF949855D689D0DD0000016ABC1AFA3B000004030047304502202B5F5E136F4242CA
6FAD463B46F00782775761963370D6E8DEC55B766BE69584022100827EB94EC95A920991442C
7B9D79BB165A61B8F2807C59E2CC6E0891F95D73460075008775BFE7597CF88C43995FBDF36E
FF568D475636FF4AB560C1B4EAFF5EA0830F0000016ABC1AFC010000040300463044022039175
4D3EEF5302242585244E3354129BFFC650E345C17BAFB7528A76924B81B0220602AD4A048E4F
C47EBF6340D89DA3A33EB60CF6153E7511A7CF8435001949893
1595:d=1 hl=2 l= 13 cons: SEQUENCE
1597:d=2 hl=2 l= 9 prim: OBJECT :sha256WithRSAEncryption
1608:d=2 hl=2 l= 0 prim: NULL
1610:d=1 hl=4 l= 257 prim: BIT STRING

[10/20/20]seed@VM:~$ openssl asn1parse -i -in c0.pem -strparse 4 -out c0_body.bin -noout
[10/20/20]seed@VM:~$ sha256sum c0_body.bin
35539711be68ceb9bf7dca53ff8e1beb36692be3be60ffbde72ac9e5078098bc c0_body.bin

5. ********** **Command** **********

[10/20/20]seed@VM:~$ gcc -o verify verify.c -lcrypto
[10/20/20]seed@VM:~$ verify
CA signature verified