

```
student@ubuntu: ~/Desktop
GNU nano 4.8 /usr/lib/ssl/misc/CA.pl
#!/usr/bin/perl
# Copyright 2000-2018 The OpenSSL Project Authors. All Rights Reserved.
#
# Licensed under the OpenSSL license (the "License"). You may not use
# this file except in compliance with the License. You can obtain a copy
# in the file LICENSE in the source distribution or at
# https://www.openssl.org/source/license.html
#
# Wrapper around the ca to make it easier to use
#
# WARNING: do not edit!
# Generated by Makefile from ../apps/CA.pl.in

use strict;
use warnings;

my $openssl = "openssl";
if(defined $ENV{'OPENSSL'}) {
    $openssl = $ENV{'OPENSSL'};
}
[ File '/usr/lib/ssl/misc/CA.pl' is unwritable ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line
```

```
student@ubuntu: ~/Desktop
Invalid backup directory: A
student@ubuntu:~/Desktop$ nano /usr/lib/ssl/misc/CA.pl -newca
student@ubuntu:~/Desktop$ /usr/lib/ssl/misc/CA.pl -newca
CA certificate filename (or enter to create)

Making CA certificate ...
====
openssl req -new -keyout ./demoCA/private/cakey.pem -out ./demoCA/careq.pem
Generating a RSA private key
.....+++++
.....+++++
writing new private key to './demoCA/private/cakey.pem'
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.
-----
Country Name (2 letter code) [AU]:in
State or Province Name (full name) [Some-State]:maharastra
```

```
s Terminal Sep 12 01:47
student@ubuntu: ~/Desktop

student@ubuntu:~/Desktop$ pwd
/home/student/Desktop
student@ubuntu:~/Desktop$ nano
student@ubuntu:~/Desktop$ nano /usr/lib/ssl/misc/ca.pl
student@ubuntu:~/Desktop$ nano /usr/lib/ssl/misc/CA.pl
student@ubuntu:~/Desktop$ nano /root/demoCA

Command 'nano' not found, did you mean:

  command 'nano' from snap nano (5.7+pkg-4057)
  command 'nama' from deb nama (1.216-1)
  command 'nana' from deb hugin-tools (2019.2.0+dfsg-1build3)
  command 'nano' from deb nano (4.8-1ubuntu1)
  command 'nant' from deb nant (0.92-rc1+dfsg-7)

See 'snap info <snapname>' for additional versions.

student@ubuntu:~/Desktop$ nano /usr/lib/ssl/openssl.cnf

Command 'nano' not found, did you mean:

  command 'nano' from snap nano (5.7+pkg-4057)
  command 'nana' from deb hugin-tools (2019.2.0+dfsg-1build3)
  command 'nant' from deb nant (0.92-rc1+dfsg-7)
  command 'nama' from deb nama (1.216-1)
  command 'nano' from deb nano (4.8-1ubuntu1)

See 'snap info <snapname>' for additional versions.

student@ubuntu:~/Desktop$ nano /usr/lib/ssl/openssl.cnf
student@ubuntu:~/Desktop$ nano /usr/lib/ssl/misc/CA.pl -newCA
Invalid backup directory: A
student@ubuntu:~/Desktop$ nano /usr/lib/ssl/misc/CA.pl -newca
student@ubuntu:~/Desktop$ /usr/lib/ssl/misc/CA.pl -newca
CA certificate filename (or enter to create)

Making CA certificate ...
=====
-----
```

```
s Terminal Sep 12 01:47
student@ubuntu: ~/Desktop

Making CA certificate ...
=====
openssl req -new -keyout ./demoCA/private/cakey.pem -out ./demoCA/careq.pem
Generating a RSA private key
.....+++++
.....+++++
writing new private key to './demoCA/private/cakey.pem'
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.
-----
Country Name (2 letter code) [AU]:in
State or Province Name (full name) [Some-State]:maharashtra^[D^[[D^[[D^[[D^[[
Locality Name (eg, city) []:mumbai
Organization Name (eg, company) [Internet Widgits Pty Ltd]:xie
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:teitxie
Email Address []:om@xie

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:teitxie
An optional company name []:om
==> 0
=====
openssl ca -create_serial -out ./demoCA/cacert.pem -days 1095 -batch -keyfile ./demoCA/private/cakey.pem -selfsign -extensions v3_ca -infil
es ./demoCA/careq.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
-----
```

```
Terminal
Sep 12 01:48
student@ubuntu: ~/Desktop

==> 0
====
====
openssl ca -create_serial -out ./demoCA/cacert.pem -days 1095 -batch -keyfile ./demoCA/private/cakey.pem -selfsign -extensions v3_ca -infil
es ./demoCA/careq.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number:
    0f:52:88:68:ea:b1:30:cd:1c:e2:c4:a5:84:76:c9:36:a0:b7:49:b9
  Validity
    Not Before: Sep 12 08:47:34 2022 GMT
    Not After : Sep 11 08:47:34 2025 GMT
  Subject:
    countryName           = in
    stateOrProvinceName   = Some-State
    organizationName      = xle
    organizationalUnitName = IT
    commonName            = teitxie
    emailAddress          = on@xie
  X509v3 extensions:
    X509v3 Subject Key Identifier:
      2B:62:2E:C8:35:11:B0:3B:6A:21:CE:44:D4:6C:D7:42:EA:3A:10:84
    X509v3 Authority Key Identifier:
      keyid:2B:62:2E:C8:35:11:B0:3B:6A:21:CE:44:D4:6C:D7:42:EA:3A:10:84
    X509v3 Basic Constraints: critical
      CA:TRUE
Certificate is to be certified until Sep 11 08:47:34 2025 GMT (1095 days)

Write out database with 1 new entries
Data Base Updated
==> 0
====
CA certificate is in ./demoCA/cacert.pem
student@ubuntu:~/Desktop$
```

```
Terminal
Sep 12 01:48
student@ubuntu: ~/Desktop

==> 0
====
====
openssl ca -create_serial -out ./demoCA/cacert.pem -days 1095 -batch -keyfile ./demoCA/private/cakey.pem -selfsign -extensions v3_ca -infil
es ./demoCA/careq.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number:
    0f:52:88:68:ea:b1:30:cd:1c:e2:c4:a5:84:76:c9:36:a0:b7:49:b9
  Validity
    Not Before: Sep 12 08:47:34 2022 GMT
    Not After : Sep 11 08:47:34 2025 GMT
  Subject:
    countryName           = in
    stateOrProvinceName   = Some-State
    organizationName      = xle
    organizationalUnitName = IT
    commonName            = teitxie
    emailAddress          = on@xie
  X509v3 extensions:
    X509v3 Subject Key Identifier:
      2B:62:2E:C8:35:11:B0:3B:6A:21:CE:44:D4:6C:D7:42:EA:3A:10:84
    X509v3 Authority Key Identifier:
      keyid:2B:62:2E:C8:35:11:B0:3B:6A:21:CE:44:D4:6C:D7:42:EA:3A:10:84
    X509v3 Basic Constraints: critical
      CA:TRUE
Certificate is to be certified until Sep 11 08:47:34 2025 GMT (1095 days)

Write out database with 1 new entries
Data Base Updated
==> 0
====
CA certificate is in ./demoCA/cacert.pem
student@ubuntu:~/Desktop$
```

```
Terminal
Sep 12 01:51
student@ubuntu: ~/Desktop/demoCA/newcerts

==> 0
====
====
openssl ca -create_serial -out ./demoCA/cacert.pem -days 1095 -batch -keyfile ./demoCA/private/cakey.pem -selfsign -extensions v3_ca -infil
es ./demoCA/cacert.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number:
    0f:52:88:68:ea:b1:30:cd:1c:e2:c4:a5:84:76:c9:36:a0:b7:49:b9
  Validity
    Not Before: Sep 12 08:47:34 2022 GMT
    Not After : Sep 11 08:47:34 2025 GMT
  Subject:
    countryName           = in
    stateOrProvinceName   = Some-State
    organizationName      = xle
    organizationalUnitName = IT
    commonName            = teitxie
    emailAddress          = om@xie
  X509v3 extensions:
    X509v3 Subject Key Identifier:
      2B:62:2E:C8:35:11:B0:3B:6A:21:CE:44:D4:6C:D7:42:EA:3A:10:84
    X509v3 Authority Key Identifier:
      keyid:2B:62:2E:C8:35:11:B0:3B:6A:21:CE:44:D4:6C:D7:42:EA:3A:10:84
    X509v3 Basic Constraints: critical
      CA:TRUE
Certificate is to be certified until Sep 11 08:47:34 2025 GMT (1095 days)

Write out database with 1 new entries
Data Base Updated
==> 0
====
CA certificate is in ./demoCA/cacert.pem
student@ubuntu: ~/Desktop$ cd demoCA/newcerts
```

```
Terminal
Sep 12 02:26
student@ubuntu: ~

Not After : Sep 12 09:24:32 2023 GMT
Subject: C=in, ST=Some-State, O=xle, OU=IT, CN=teitxie/emailAddress=om66@xieit
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public-Key: (2048 bit)
  Modulus:
    00:f3:bb:32:e6:90:92:21:9b:75:55:ec:75:06:ac:
    57:d0:39:98:b1:3e:34:f8:00:86:d7:23:b5:38:98:
    6c:b6:2b:f8:8a:2c:06:57:71:14:28:bd:97:db:73:
    64:42:b5:c2:88:34:38:07:af:fd:2a:ee:25:64:5b:
    ef:ca:ec:79:06:82:28:e6:31:48:3e:43:af:7d:0f:
    19:42:0a:ca:cd:29:c5:b5:51:d8:34:78:24:ef:a0:
    b0:a6:a3:02:2c:80:02:1d:9d:35:ab:92:2d:99:85:
    8e:16:ff:e6:30:e0:ec:bd:a3:3c:48:5a:f8:32:e5:
    4f:e7:e0:08:ce:d5:76:7a:b5:a2:22:fb:3f:f7:53:
    3c:c1:75:c8:f9:80:7a:e8:6c:3f:40:d4:fc:de:9a:
    3c:f3:8d:01:49:d6:c6:37:3c:1a:f8:27:9e:38:73:
    64:ba:3f:6a:e5:f2:23:82:9e:9f:b6:56:b8:08:01:
    95:8a:bb:e0:66:6a:28:95:fd:5d:72:51:f8:ba:9d:
    fb:f8:7b:fe:dd:4d:ea:3b:ae:af:f3:a5:a7:e0:40:
    d9:13:55:78:d4:5e:0c:47:75:e7:a7:8d:d7:ff:17:
    43:c7:54:71:7a:11:c7:48:97:a2:86:e3:36:4f:ff:
    a1:10:ad:b5:58:71:36:5e:89:df:2c:15:29:34:dc:
    65:c3
  Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
  Netscape Comment:
    OpenSSL Generated Certificate
  X509v3 Subject Key Identifier:
    8B:BC:E8:0E:B5:0C:AA:0C:1F:EA:CC:CE:3B:8F:F4:A6:37:32:7F:C9
  X509v3 Authority Key Identifier:
    keyid:2B:62:2E:C8:35:11:B0:3B:6A:21:CE:44:D4:6C:D7:42:EA:3A:10:84

Signature Algorithm: sha256WithRSAEncryption
49:9d:4e:29:ab:50:48:4e:7d:00:45:ce:13:81:8e:bd:9a:c1:
e0:1c:6d:c4:ca:6c:a6:74:d8:62:5b:66:9f:55:99:9b:ff:09:
41:61:47:80:41:51:93:46:64:40:08:20:23:21:66:08:63:61:
```

```
Terminal
Sep 12 02:26
student@ubuntu: ~

49:9d:4e:29:ab:50:48:4e:7d:00:45:ce:13:81:8e:bd:9a:c1:
e0:1c:6d:c4:ca:6c:a6:74:d8:62:5b:66:9f:55:99:9b:ff:09:
de:fc:47:88:d4:54:72:46:f1:49:d9:29:c3:24:16:c0:52:f1:
be:eb:51:3e:77:11:7f:7c:8a:a9:bc:14:93:7b:71:53:94:a9:
88:21:e2:ea:77:ff:63:ba:d1:76:7a:e7:43:75:ba:9d:c2:8a:
c8:f8:82:43:8b:57:61:ac:cf:3d:bb:35:3c:fa:a7:fc:1d:98:
3d:d0:8c:91:7e:7b:bb:ee:e1:4b:3a:f8:97:04:23:db:75:b5:
97:8a:16:44:a9:bd:da:31:19:36:8a:02:18:e9:42:1a:03:0a:
95:80:b2:3a:1c:4d:f3:24:a6:48:a4:eb:de:a4:a8:6e:7b:3e:
cb:29:4f:55:ec:90:5e:d9:28:98:0a:cb:32:9e:8a:0a:c7:a1:
15:86:47:47:19:91:7e:7e:0f:6f:93:2f:22:98:80:eb:14:
41:e8:f7:50:7d:57:48:f8:ab:45:56:be:ba:55:13:16:8d:bc:
a0:2f:97:54:37:dd:8e:44:35:b2:0c:cc:65:70:e4:51:70:ae:
eb:f2:28:3f:db:5b:e9:fe:dc:ba:75:a9:88:0f:de:3b:ef:3c:
97:00:08:d0
-----BEGIN CERTIFICATE-----
MIID2TCCAsGgAwIBAgIUd1KIaOqxMM0c4s5LhHbJNqC3SbowDQYJKoZIhvcNAQEL
BQAwZjELMAkGA1UEBhMCaW4xEzARBgNVBAgMClnvbmU3RhdGxhDAAKBgNVBAoM
A3hpZTELMAkGA1UECwwCSVQxEDAOBgNVBAcMB3RlaxR4aWUxFTATBgkqhkiG9w0B
CQEWBm9tQHhpZTAeFw0yMjA5MTIwOTI0MzJaFw0yMzA5MTIwOTI0MzJaMGoxCzAJ
BgNVBAYTAmluMRMwEQYDVQIDABTb211LVN0YXRlMQwwCgYDVQQKDAN4aWUxCzAJ
BgNVBAsMAklUMRAwDgYDVQQDDAd0ZWl0eGllMRkwFwYJKoZIhvcNAQk8FgpvBTY2
QHhpZk10MjI1IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA87sySpC5IZt1
Vex1BqxX0dmYsT40+ACC1yO10JhstL44CAGVlrvGZmo0Lf1dcLH4up37+Hv+3U3q
ZFvvyux5BoIo5JfIPkOvFQ8ZQgrKzSnFtVHYNHqK76CwpqMCLIAChZ01q5ItmVW0
Fv/mMODSvaM85Fr4MuVP5+AlztV2erWlIvs/91M8wXXI+YB66Gw/QNT83po8840B
SdbGNzwa+CeeOHnKuj9q5fIjgp6fTL4CAGVlrvGZmo0Lf1dcLH4up37+Hv+3U3q
066v86Wn4EDZE1V41F4MR3Xnp43X/xd0x1RxeHHSJeLhuM2T/+hEK21WHE2Xonf
LBUpNNXlwwIDAQABo3sweTAJBgNVHRMEAIAAMCwGCWCGSAGG+EIBDQ0FFh1PcGVu
U1NMIEEdLbmVvYXRlZCB0ZXJ0aWZpY2F0ZTAuBgNVHQ4EFgQUi7zoDrUMggwF6sZ0
04/0pjcyf8kWhwYDVROjBBgwFoAUKZiuyDURSdtqIC5E1GzXQuo6EIQwDQYJKoZI
hvcNAQELBQADggEBAAEmdTmrUEhOFQBFzh0Bjr2aweAcBcTKbKZ02GJbZp9VnZv/
Cd78R4jUVHJG8UnZKcMkF5BS8b7rUT53EX98lqm8FJN7cV0UqYgh4up3/2060XZ6
58N1up3C1sJ4gkOLV2Gsz27NTz6p/wdmD3QjJF+e7vu4Us6+JcEI9t1tZekFkSp
vdoxGTaKAhjpQh0DCpWASjocTFMkpklk696kqG57PsspT1XskF7ZKJgKyzKeLgrH
oRWGR0cZkX5+fg9vky8ImIDrFEHo9189V0j4q0VlvrvPvEXaHvKAvL1JQ33Y5ENbIM
zGVw5FFwruvyKD/bW+n+3Lp1qYgP3jvvpJcACNA=
-----END CERTIFICATE-----
```

View file

Sep 12 02:34

0F528868EAB130CD1CE2C4A58476C936A0B749B9.pem

teitxie

Identity: teitxie

Verified by: teitxie

Expires: 09/11/2025

Details

Subject Name

C (Country): in

ST (State): Some-State

O (Organization): xie

OU (Organizational Unit): IT

CN (Common Name): teitxie

EMAIL (Email Address): om@xie

Issuer Name

C (Country): in

ST (State): Some-State

O (Organization): xie

OU (Organizational Unit): IT

CN (Common Name): teitxie

EMAIL (Email Address): om@xie

Issued Certificate

Version: 3

Serial Number: 0F 52 88 68 EA B1 30 CD 1C E2 C4 A5 84 76 C9 36 A0 B7 49 B9

Not Valid Before: 2022-09-12

Not Valid After: 2025-09-11

Certificate Fingerprints

SHA1: 02 9C 59 27 DD 1A 33 53 EE E2 D6 4F 02 52 9B C5 55 16 5A 24

MD5: 79 C5 F6 EF A2 10 7B 79 CF 89 2E A6 18 72 6F A9

Public Key Info

Key Algorithm: RSA

Close

Import

View file

Sep 12 02:34

0F528868EAB130CD1CE2C4A58476C936A0B749B9.pem

Public Key Info

Key Algorithm: RSA

Key Parameters: 05 00

Key Size: 2048

Key SHA1 Fingerprint: ED 0E D9 11 67 FF 7E 7D 79 B5 43 28 F8 43 69 72 AD B0 1A 36

Public Key: 30 82 01 0A 02 82 01 01 00 C7 32 98 DB 58 BF AD 85 49 45 BA 76 F4 0D 27 CC 86 28 0E 4F DE D1 FF F3 49 BF 83 C0 54 C0 A8 E2 55 F5 23 D4 48 88 7A A1 41 C5 32 EA 1E 78 E2 30 B4 3D A0 6D 47 C4 4B 91 6F 6B 1E 57 BD 79 2D EF D3 9A 19 62 4A D4 2E 70 52 92 BF 7F CA 9D 90 25 58 9E 46 16 AD E0 C1 53 DC 2C 05 59 1A AF E0 CE 14 53 2C 46 3D A2 12 93 B9 7D 04 EF AC 45 B1 A7 A2 8D 85 B7 FE BE 80 E4 55 8E 78 FE C3 39 72 AF C1 EE 32 AB C9 F9 47 8A E4 9C B3 7B 7A 14 09 86 1E A7 84 D1 6A F4 C2 F6 DF E8 D8 01 FB E0 7F 46 33 B7 DB 11 7E 67 A0 AA 97 28 7F 5E 10 B8 E3 50 3E 04 3D BC CA 9D 1C 69 AB CC 6E FD D8 66 BC E3 6E 94 E3 A6 E1 8E F6 E2 2F D6 2A 44 B1 94 8D 25 50 E9 C2 6C D8 04 B3 46 F3 4B B6 AF 69 5D 22 8F BC 57 B4 21 7D D9 CF 16 A6 34 F2 87 6E 1E 58 8F FA 9F 3E 6C 50 C9 BD 01 31 41 80 90 9F 74 04 69 02 03 01 00 01

Subject Key Identifier

Key Identifier: 2B 62 2E C8 35 11 B0 3B 6A 21 CE 44 D4 6C D7 42 EA 3A 10 84

Critical: No

Extension

Identifier: 2.5.29.35

Value: 30 16 80 14 2B 62 2E C8 35 11 B0 3B 6A 21 CE 44 D4 6C D7 42 EA 3A 10 84

Critical: No

Basic Constraints

Certificate Authority: Yes

Max Path Length: Unlimited

Critical: Yes

Signature

Signature Algorithm: 1.2.840.113549.1.1.11

Signature Parameters: 05 00

Signature: C6 AB 16 F9 F0 22 A3 B1 13 73 0E 92 B9 03 46 B8 2E F4 46 CB 5E 0D 7F B7 EB EA 03 58 37 10 25 25 27 F2 11 5A A9 DC 2A 6E 95 51 E9 2F 25 9A CF E8 DE FD F5 DD 73 EC BA 4A 73 16 F1 D0 62 E2 F7 02 11 3F 66 B8 33 CA 92 14 6C 31 B5 AD AB 97 08 7E 1C 55 44 A7 86 98 42 C2 CF CB AA 88 65 97 80 8B 39 96 49 9A 2D 26 17 25 D1 95 A2 3A 81 D2 25 E0 64 4F E0 A7 C2 0A C7 5B 73 26 96 C6 E2 B1 C4 4E B2 33 9D EB 36 62 76 0E F9 77 F1 6E 03 34 D1 64 97 DF 28 5E 43 08 E6 D7 3F 31 25 FD CA A9 54 78 5B A6 CE 00 AA B5 41 C7 FA 46 D1 F8 1B FA BB 3D 54 B0 6E E7 24 42 45 A4 0F 34 48 3C 58 3D FF 70 F8 37 R6 28 D1 D7 7E 4C 5B A6 CE 00 AA B5 41 C7 FA 46 D1 F8 1B FA BB 3D 54 B0 6E E7 24 42 45 A4 0F 34 48 3C 58 3D FF 70 F8 37 R6 28 D1 D7 7E 4C

Close

Import

View file

Sep 12 02:34

0F528868EAB130CD1CE2C4A58476C936A0B749B9.pem

Key Size: 2048

Key SHA1 Fingerprint: ED 0E D9 11 67 FF 7E 7D 79 B5 43 28 F8 43 69 72 AD B0 1A 36

Public Key: 30 82 01 0A 02 82 01 01 00 C7 32 98 DB 58 BF AD 85 49 45 BA 76 F4 0D 27 CC 86 28 0E 4F DE D1 FF F3 49 BF 83 C0 54 C0 A8 E2 55 F5 23 D4 48 88 7A A1 41 C5 32 EA 1E 78 E2 30 B4 3D A0 6D 47 C4 4B 91 6F 6B 1E 57 BD 79 2D EF D3 9A 19 62 4A D4 2E 70 52 92 BF 7F CA 9D 90 25 58 9E 46 16 AD E0 C1 53 DC 2C 05 59 1A AF E0 CE 14 53 2C 46 3D A2 12 93 B9 7D 04 EF AC 45 B1 A7 A2 8D 85 B7 FE BE 80 E4 55 8E 78 FE C3 39 72 AF C1 EE 32 AB C9 F9 47 8A E4 9C B3 7B 7A 14 09 86 1E A7 84 D1 6A F4 C2 F6 DF E8 D8 01 FB E0 7F 46 33 B7 DB 11 7E 67 A0 AA 97 28 7F 5E 10 B8 E3 50 3E 04 3D BC CA 9D 1C 69 AB CC 6E FD D8 66 BC E3 6E 94 E3 A6 E1 8E F6 E2 2F D6 2A 44 B1 94 8D 25 50 E9 C2 6C D8 04 B3 46 F3 4B B6 AF 69 5D 22 8F BC 57 B4 21 7D D9 CF 16 A6 34 F2 87 6E 1E 58 8F FA 9F 3E 6C 50 C9 BD 01 31 41 80 90 9F 74 04 69 02 03 01 00 01

Subject Key Identifier

Key Identifier: 2B 62 2E C8 35 11 B0 3B 6A 21 CE 44 D4 6C D7 42 EA 3A 10 84

Critical: No

Extension

Identifier: 2.5.29.35

Value: 30 16 80 14 2B 62 2E C8 35 11 B0 3B 6A 21 CE 44 D4 6C D7 42 EA 3A 10 84

Critical: No

Basic Constraints

Certificate Authority: Yes

Max Path Length: Unlimited

Critical: Yes

Signature

Signature Algorithm: 1.2.840.113549.1.1.11

Signature Parameters: 05 00

Signature: C6 AB 16 F9 F0 22 A3 B1 13 73 0E 92 B9 03 46 B8 2E F4 46 CB 5E 0D 7F B7 EB EA 03 58 37 10 25 25 27 F2 11 5A A9 DC 2A 6E 95 51 E9 2F 25 9A CF E8 DE FD F5 DD 73 EC BA 4A 73 16 F1 D0 62 E2 F7 02 11 3F 66 B8 33 CA 92 14 6C 31 B5 AD AB 97 08 7E 1C 55 44 A7 86 98 42 C2 CF CB AA 88 65 97 80 8B 39 96 49 9A 2D 26 17 25 D1 95 A2 3A 81 D2 25 E0 64 4F E0 A7 C2 0A C7 5B 73 26 96 C6 E2 B1 C4 4E B2 33 9D EB 36 62 76 0E F9 77 F1 6E 03 34 D1 64 97 DF 28 5E 43 08 E6 D7 3F 31 25 FD CA A9 54 78 5B A6 CE 00 AA B5 41 C7 FA 46 D1 F8 1B FA BB 3D 54 B0 6E E7 24 42 45 A4 0F 34 48 3C 58 3D FF 70 F8 37 R6 28 D1 D7 7E 4C 92 14 58 FB 60 34 21 78 F6 B2 3F 0C 2A 4A FE 63 BC 9C 29 84 2E 88 D0 1C 3B 9B 83 8B 86 D3 6A 25 74 A4 A1 A4 07 17 E9 86 CE 2B 40 0A 68 A8 B5 8D 09 14 0C 03 4B 59 F2 66

Close

Import