East West University

Title: SECURING A NETWORKED SYSTEM WITH PUBLIC KEY INFRASTRUCTURE

GROUP : 14

PRESENTED BY

Prinom Mozumder (2021-2-60-098)

Rokeya Jahan Chowdhury Ettifa (2020-1-60-232)

Tasnim Israk Synthia(2021-2-60-097)

Umme Atika Borsha(2021-2-60-076)

PRESENTED TO

Dr. Md. Hasanul Ferdaus
Assistant Professor
Department of Computer Science and Engineering

Introduction

Page 03

- Importance and significance of Public Key Infrastructure (PKI)
- Key components of PKI
- Ensuring security using PKI

Objective

- Authentication
- Data Integrity
- Confidentiality
- Secure Key Management
- Resilience Against Cyber Threats
- Access Control
- Secure Web Traffic
- Secure Network Communication

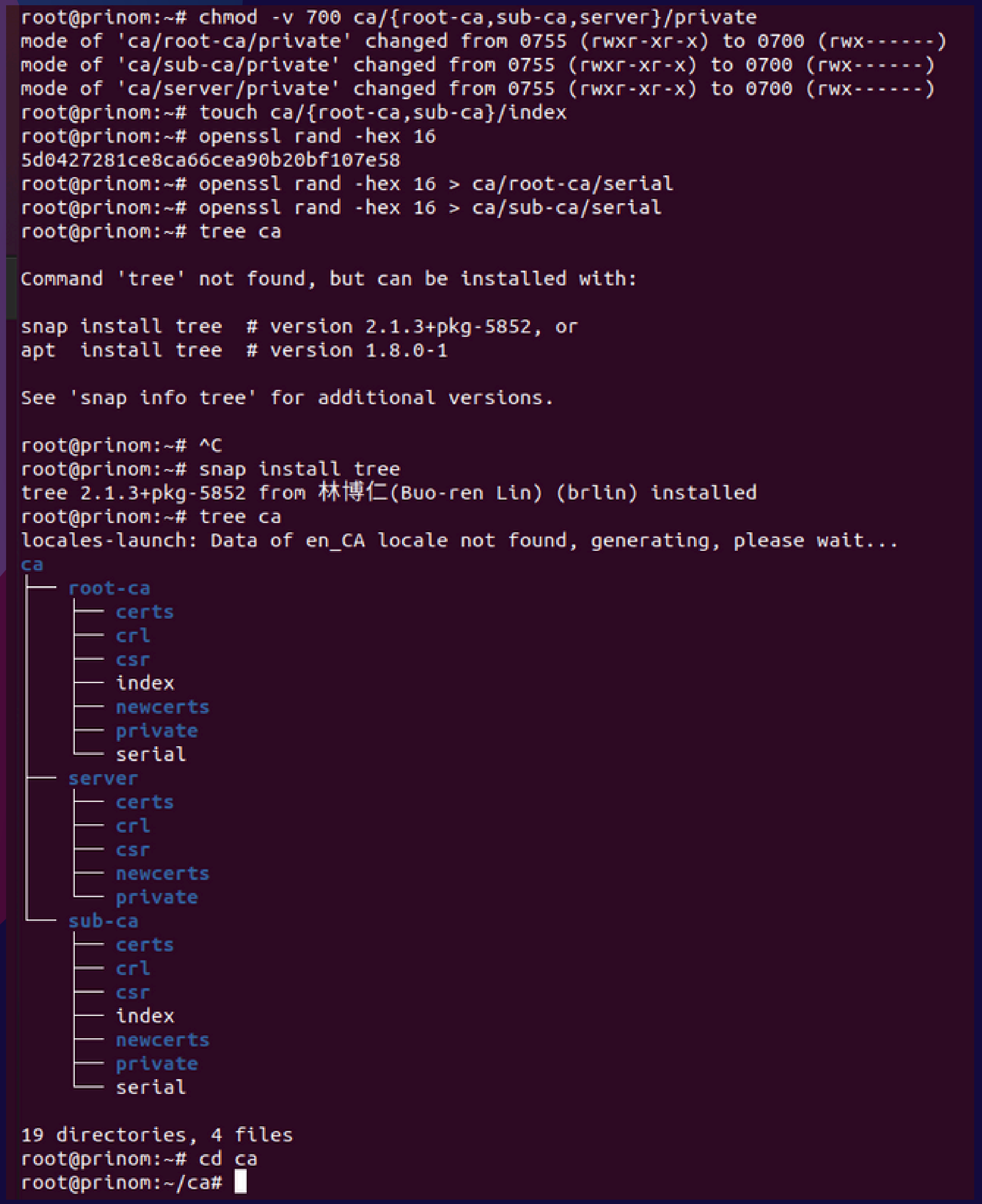
Page 05

Public Key Infrustucture

- Configuration of Certification Authority AcmeCA with AcmeRootCA as the RootCA.
- Configuration of the Web Server with Apache2 on a Linux Host.
- CSR Configuration and Generation for the www.verysecureserver.com
- Transferring the CSR to AcmeCA.
- Certification process (Verification and Certificate Generation from CSR)
- Transferring the certificate from AcmeCA to www.verysecureserver.com
- Installation of the signed the SSL certificate in the server www.verysecureserver.com
- Making the system trust Acme-RootCA

IMPLEMENTATION STEPS

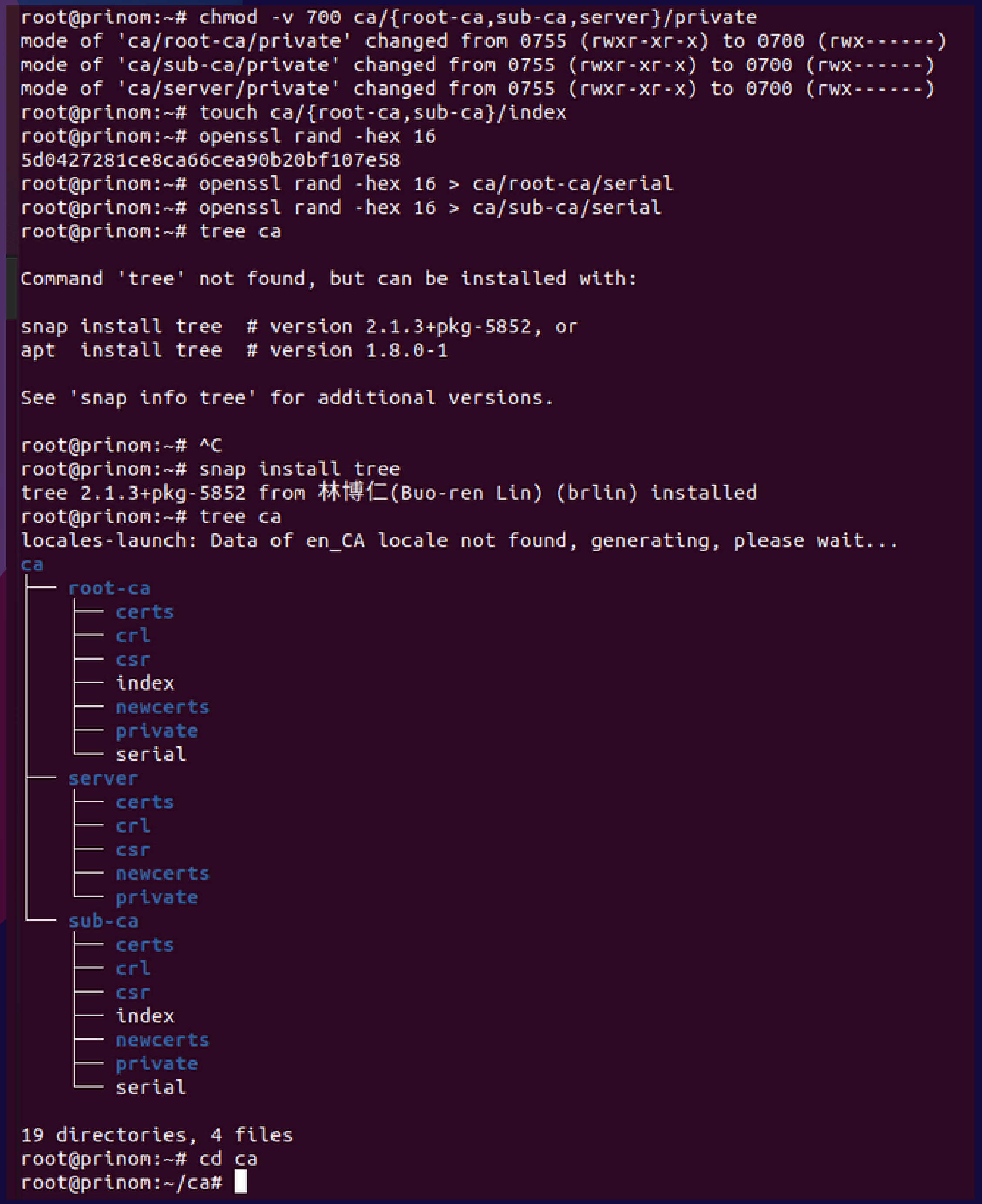
Preparing the environment



```
root@prinom:~# chmod -v 700 ca/{root-ca,sub-ca,server}/private
mode of 'ca/root-ca/private' changed from 0755 (rwxr-xr-x) to 0700 (rwx------)
mode of 'ca/sub-ca/private' changed from 0755 (rwxr-xr-x) to 0700 (rwx------)
mode of 'ca/server/private' changed from 0755 (rwxr-xr-x) to 0700 (rwx------)
root@prinom:~# touch ca/{root-ca,sub-ca}/index
root@prinom:~# openssl rand -hex 16
5d0427281ce8ca66cea90b20bf107e58
root@prinom:~# openssl rand -hex 16 > ca/root-ca/serial
root@prinom:~# openssl rand -hex 16 > ca/sub-ca/serial
root@prinom:~# tree ca

Command 'tree' not found, but can be installed with:

snap install tree  # version 2.1.3+pkg-5852, or
apt  install tree  # version 1.8.0-1

See 'snap info tree' for additional versions.

root@prinom:~# ^C
root@prinom:~# snap install tree
tree 2.1.3+pkg-5852 from 林博仁(Buo-ren Lin) (brlin) installed
root@prinom:~# tree ca
locales-launch: Data of en_CA locale not found, generating, please wait...
ca
├── root-ca
│   ├── certs
│   ├── crl
│   ├── csr
│   ├── index
│   ├── newcerts
│   ├── private
│   └── serial
├── server
│   ├── certs
│   ├── crl
│   ├── csr
│   ├── newcerts
│   └── private
└── sub-ca
    ├── certs
    ├── crl
    ├── csr
    ├── index
    ├── newcerts
    ├── private
    └── serial

19 directories, 4 files
root@prinom:~# cd ca
root@prinom:~/ca# 
```

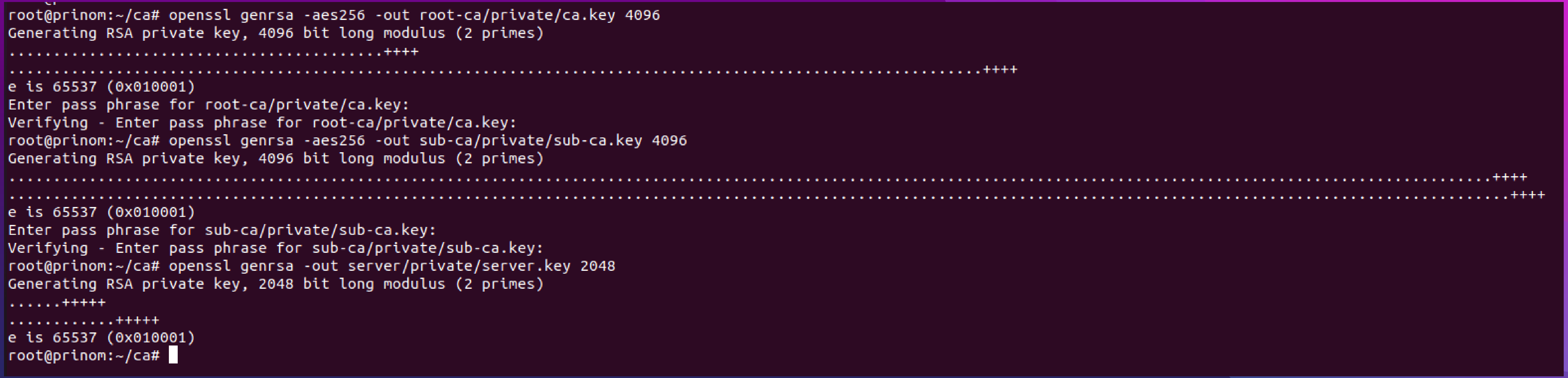
IMPLEMENTATION STEPS

Preparing the environment



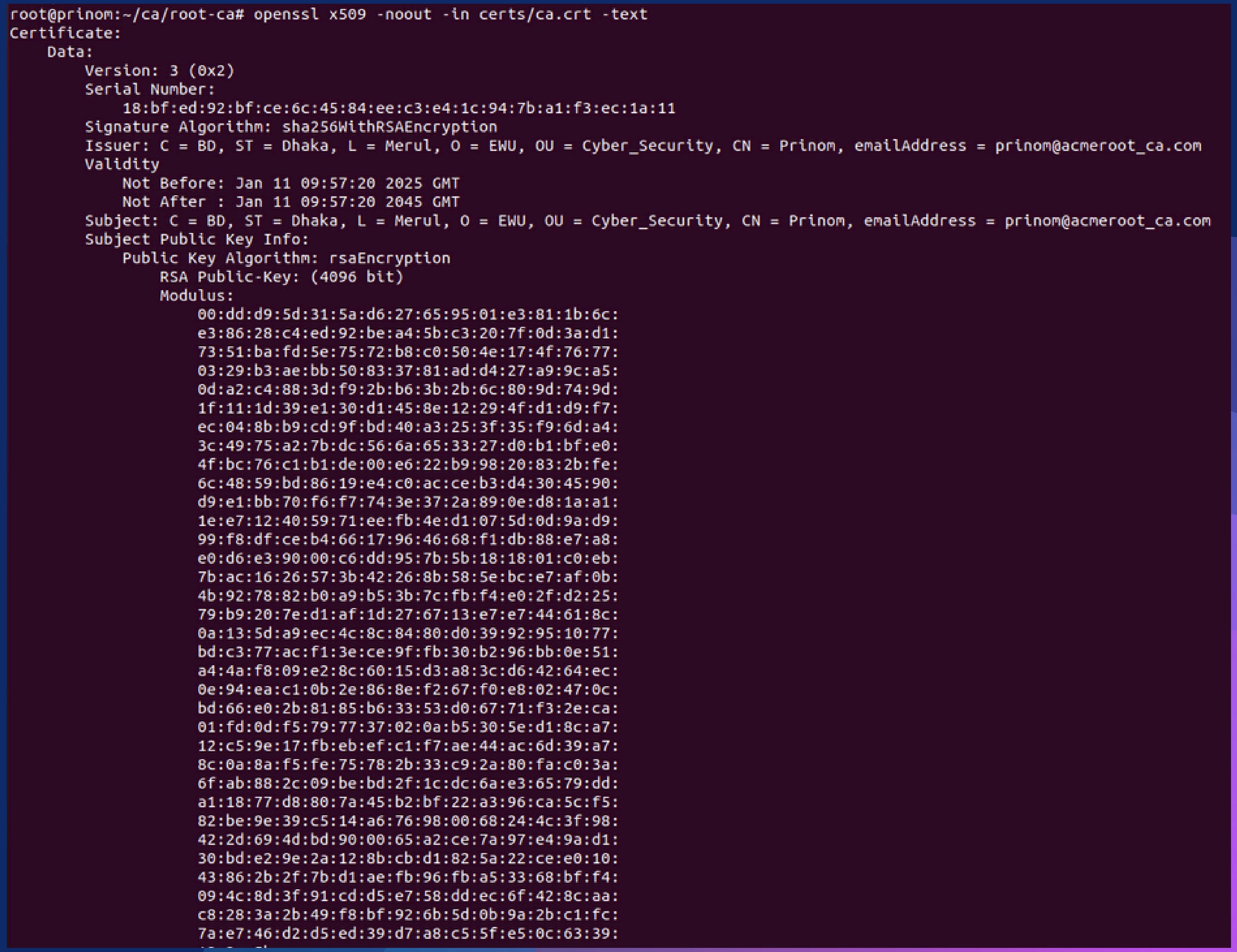
```
root@prinom:~# chmod -v 700 ca/{root-ca,sub-ca,server}/private
mode of 'ca/root-ca/private' changed from 0755 (rwxr-xr-x) to 0700 (rwx------)
mode of 'ca/sub-ca/private' changed from 0755 (rwxr-xr-x) to 0700 (rwx------)
mode of 'ca/server/private' changed from 0755 (rwxr-xr-x) to 0700 (rwx------)
root@prinom:~# touch ca/{root-ca,sub-ca}/index
root@prinom:~# openssl rand -hex 16
5d0427281ce8ca66cea90b20bf107e58
root@prinom:~# openssl rand -hex 16 > ca/root-ca/serial
root@prinom:~# openssl rand -hex 16 > ca/sub-ca/serial
root@prinom:~# tree ca

Command 'tree' not found, but can be installed with:

snap install tree  # version 2.1.3+pkg-5852, or
apt  install tree  # version 1.8.0-1

See 'snap info tree' for additional versions.

root@prinom:~# ^C
root@prinom:~# snap install tree
tree 2.1.3+pkg-5852 from 林博仁(Buo-ren Lin) (brlin) installed
root@prinom:~# tree ca
locales-launch: Data of en_CA locale not found, generating, please wait...
ca
├── root-ca
│   ├── certs
│   ├── crl
│   ├── csr
│   ├── index
│   ├── newcerts
│   ├── private
│   └── serial
├── server
│   ├── certs
│   ├── crl
│   ├── csr
│   ├── newcerts
│   └── private
└── sub-ca
    ├── certs
    ├── crl
    ├── csr
    ├── index
    ├── newcerts
    ├── private
    └── serial

19 directories, 4 files
root@prinom:~# cd ca
root@prinom:~/ca#
```

Generating private key for root ca, sub ca and server



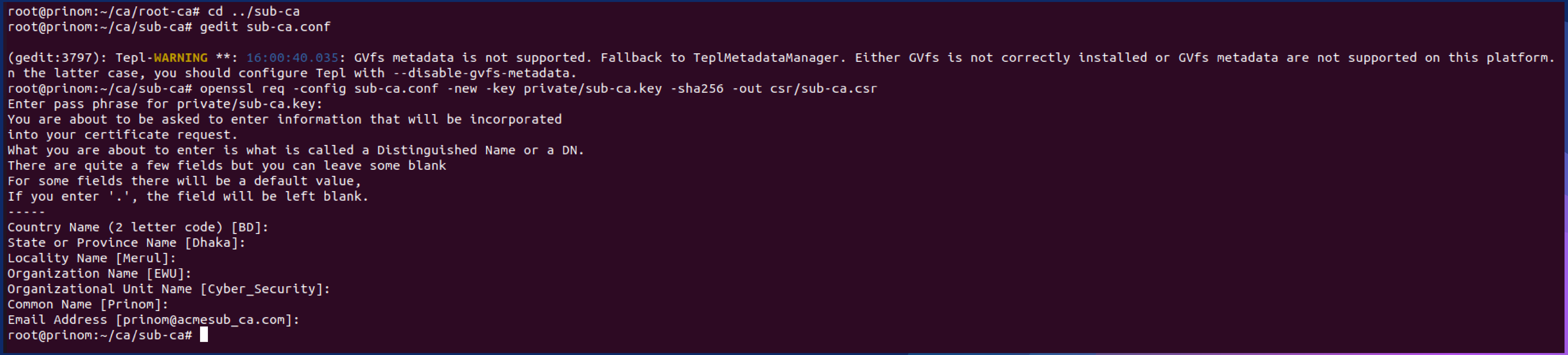
```
root@prinom:~/ca# openssl genrsa -aes256 -out root-ca/private/ca.key 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
..........................................++++
.............................................................................................................++++
e is 65537 (0x010001)
Enter pass phrase for root-ca/private/ca.key:
Verifying - Enter pass phrase for root-ca/private/ca.key:
root@prinom:~/ca# openssl genrsa -aes256 -out sub-ca/private/sub-ca.key 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
......................................................................................................................................................................++++
........................................................................................................................................................................++++
e is 65537 (0x010001)
Enter pass phrase for sub-ca/private/sub-ca.key:
Verifying - Enter pass phrase for sub-ca/private/sub-ca.key:
root@prinom:~/ca# openssl genrsa -out server/private/server.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
......+++++
............+++++
e is 65537 (0x010001)
root@prinom:~/ca# 
```

Ensuring that the certificate has been created properly



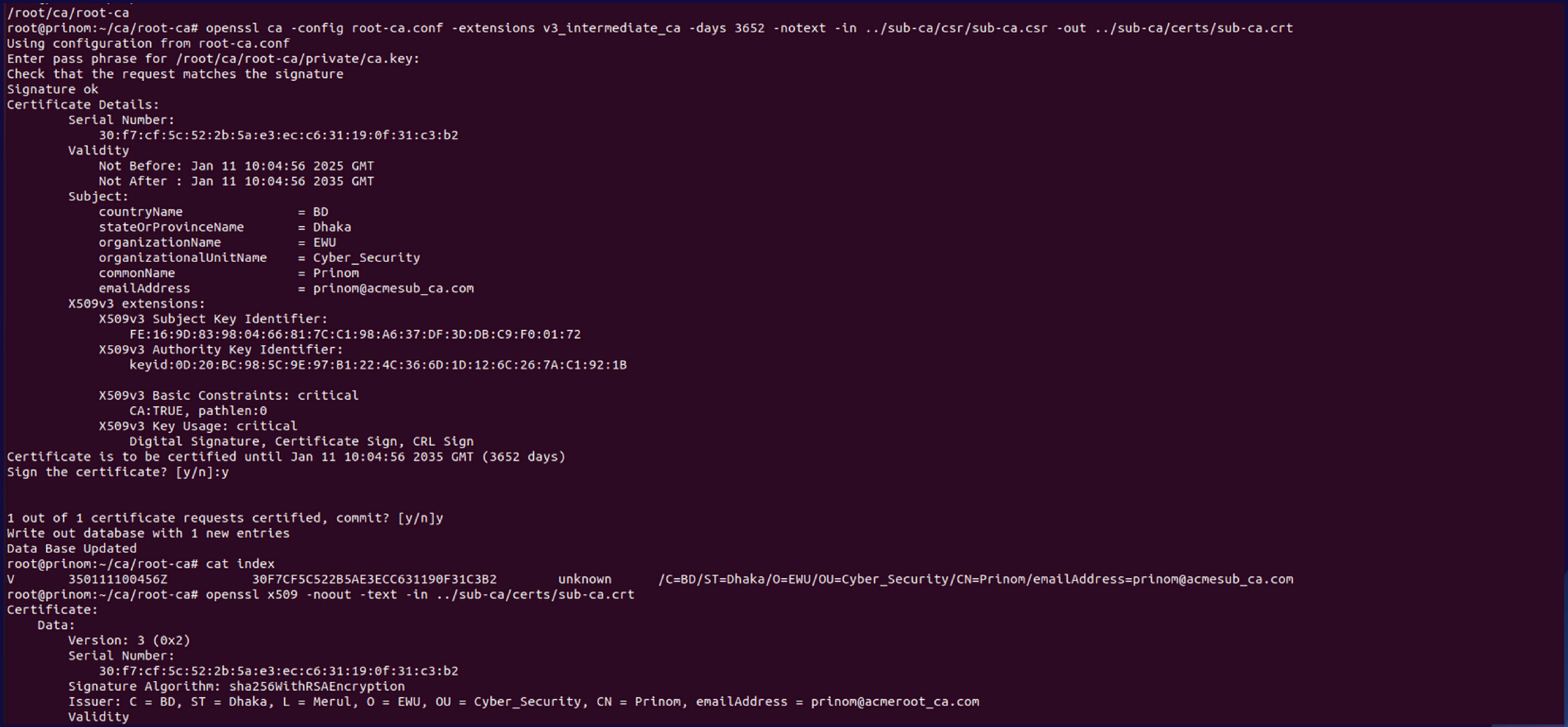
```
root@prinom:~/ca/root-ca# openssl x509 -noout -in certs/ca.crt -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            18:bf:ed:92:bf:ce:6c:45:84:ee:c3:e4:1c:94:7b:a1:f3:ec:1a:11
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = BD, ST = Dhaka, L = Merul, O = EWU, OU = Cyber_Security, CN = Prinom, emailAddress = prinom@acmeroot_ca.com
        Validity
            Not Before: Jan 11 09:57:20 2025 GMT
            Not After : Jan 11 09:57:20 2045 GMT
        Subject: C = BD, ST = Dhaka, L = Merul, O = EWU, OU = Cyber_Security, CN = Prinom, emailAddress = prinom@acmeroot_ca.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:dd:d9:5d:31:5a:d6:27:65:95:01:e3:81:1b:6c:
                    e3:86:28:c4:ed:92:be:a4:5b:c3:20:7f:0d:3a:d1:
                    73:51:ba:fd:5e:75:72:b8:c0:50:4e:17:4f:76:77:
                    03:29:b3:ae:bb:50:83:37:81:ad:d4:27:a9:9c:a5:
                    0d:a2:c4:88:3d:f9:2b:b6:3b:2b:6c:80:9d:74:9d:
                    1f:11:1d:39:e1:30:d1:45:8e:12:29:4f:d1:d9:f7:
                    ec:04:8b:b9:cd:9f:bd:40:a3:25:3f:35:f9:6d:a4:
                    3c:49:75:a2:7b:dc:56:6a:65:33:27:d0:b1:bf:e0:
                    4f:bc:76:c1:b1:de:00:e6:22:b9:98:20:83:2b:fe:
                    6c:48:59:bd:86:19:e4:c0:ac:ce:b3:d4:30:45:90:
                    d9:e1:bb:70:f6:f7:74:3e:37:2a:89:0e:d8:1a:a1:
                    1e:e7:12:40:59:71:ee:fb:4e:d1:07:5d:0d:9a:d9:
                    99:f8:df:ce:b4:66:17:96:46:68:f1:db:88:e7:a8:
                    e0:d6:e3:90:00:c6:dd:95:7b:5b:18:18:01:c0:eb:
                    7b:ac:16:26:57:3b:42:26:8b:58:5e:bc:e7:af:0b:
                    4b:92:78:82:b0:a9:b5:3b:7c:fb:f4:e0:2f:d2:25:
                    79:b9:20:7e:d1:af:1d:27:67:13:e7:e7:44:61:8c:
                    0a:13:5d:a9:ec:4c:8c:84:80:d0:39:92:95:10:77:
                    bd:c3:77:ac:f1:3e:ce:9f:fb:30:b2:96:bb:0e:51:
                    a4:4a:f8:09:e2:8c:60:15:d3:a8:3c:d6:42:64:ec:
                    0e:94:ea:c1:0b:2e:86:8e:f2:67:f0:e8:02:47:0c:
                    bd:66:e0:2b:81:85:b6:33:53:d0:67:71:f3:2e:ca:
                    01:fd:0d:f5:79:77:37:02:0a:b5:30:5e:d1:8c:a7:
                    12:c5:9e:17:fb:eb:ef:c1:f7:ae:44:ac:6d:39:a7:
                    8c:0a:8a:f5:fe:75:78:2b:33:c9:2a:80:fa:c0:3a:
                    6f:ab:88:2c:09:be:bd:2f:1c:dc:6a:e3:65:79:dd:
                    a1:18:77:d8:80:7a:45:b2:bf:22:a3:96:ca:5c:f5:
                    82:be:9e:39:c5:14:a6:76:98:00:68:24:4c:3f:98:
                    42:2d:69:4d:bd:90:00:65:a2:ce:7a:97:e4:9a:d1:
                    30:bd:e2:9e:2a:12:8b:cb:d1:82:5a:22:ce:e0:10:
                    43:86:2b:2f:7b:d1:ae:fb:96:fb:a5:33:68:bf:f4:
                    09:4c:8d:3f:91:cd:d5:e7:58:dd:ec:6f:42:8c:aa:
                    c8:28:3a:2b:49:f8:bf:92:6b:5d:0b:9a:2b:c1:fc:
                    7a:e7:46:d2:d5:ed:39:d7:a8:c5:5f:e5:0c:63:39:
```

Requesting for sub ca certificate signing request



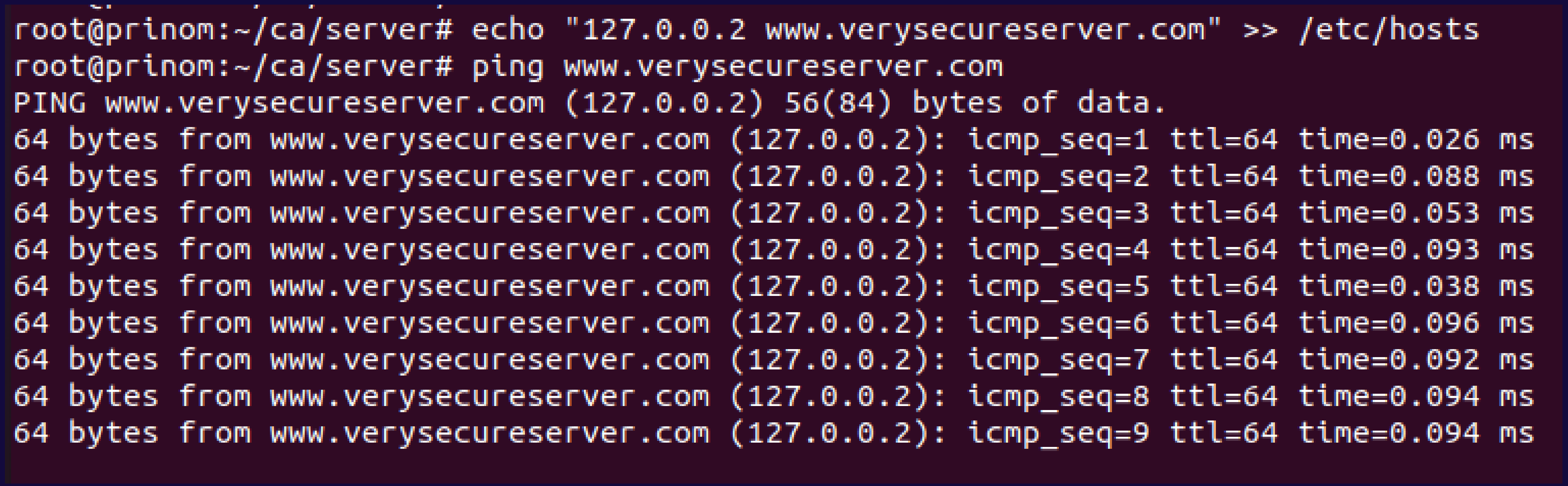
```
root@prinom:~/ca/root-ca# cd ../sub-ca
root@prinom:~/ca/sub-ca# gedit sub-ca.conf

(gedit:3797): Tepl-WARNING **: 16:00:40.035: GVfs metadata is not supported. Fallback to TeplMetadataManager. Either GVfs is not correctly installed or GVfs metadata are not supported on this platform.
n the latter case, you should configure Tepl with --disable-gvfs-metadata.
root@prinom:~/ca/sub-ca# openssl req -config sub-ca.conf -new -key private/sub-ca.key -sha256 -out csr/sub-ca.csr
Enter pass phrase for private/sub-ca.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.
-----
Country Name (2 letter code) [BD]:
State or Province Name [Dhaka]:
Locality Name [Merul]:
Organization Name [EWU]:
Organizational Unit Name [Cyber_Security]:
Common Name [Prinom]:
Email Address [prinom@acmesub_ca.com]:
root@prinom:~/ca/sub-ca# 
```

Configuring server



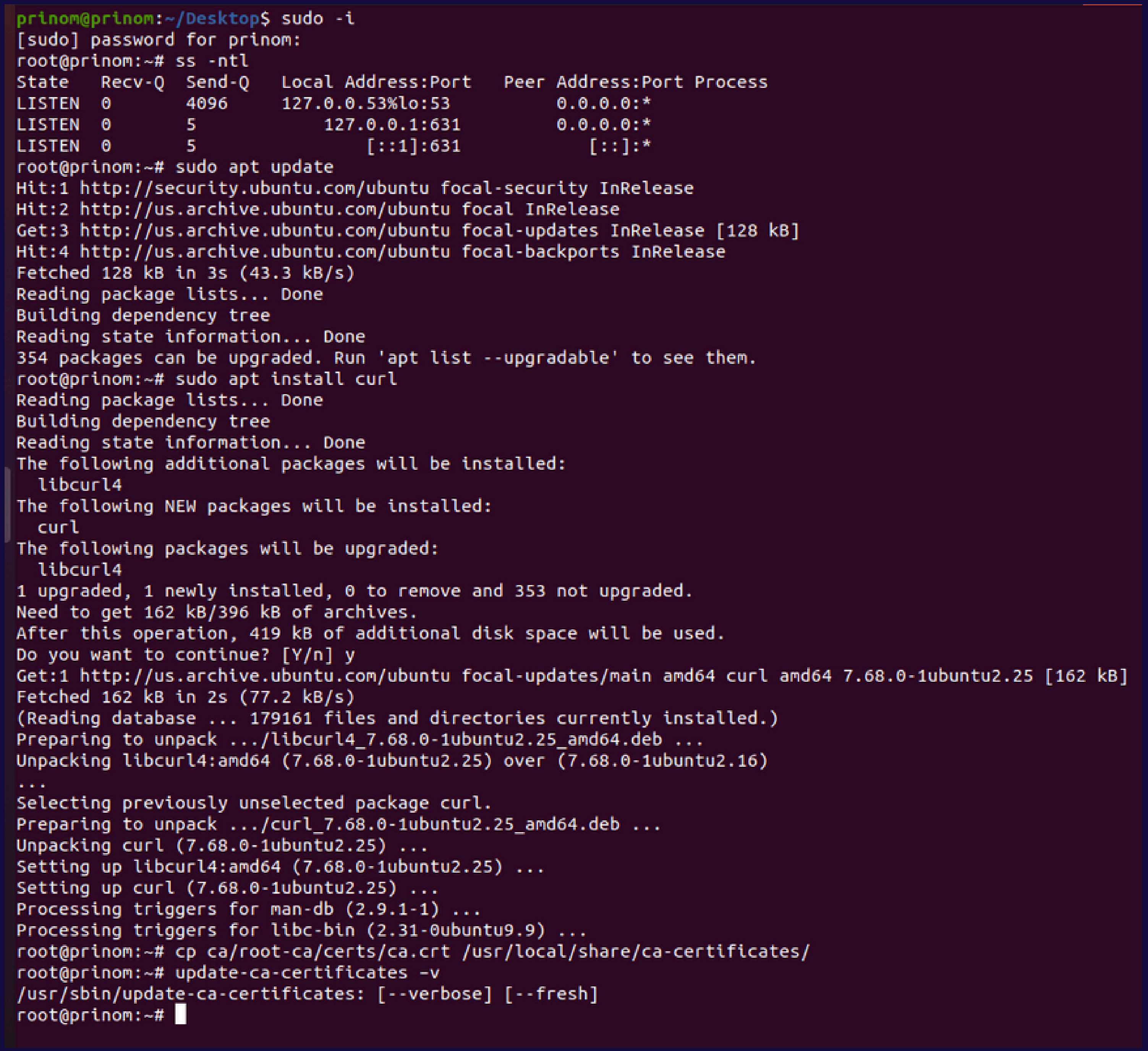
```
/root/ca/root-ca
root@prinom:~/ca/root-ca# openssl ca -config root-ca.conf -extensions v3_intermediate_ca -days 3652 -notext -in ../sub-ca/csr/sub-ca.csr -out ../sub-ca/certs/sub-ca.crt
Using configuration from root-ca.conf
Enter pass phrase for /root/ca/root-ca/private/ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            30:f7:cf:5c:52:2b:5a:e3:ec:c6:31:19:0f:31:c3:b2
        Validity
            Not Before: Jan 11 10:04:56 2025 GMT
            Not After : Jan 11 10:04:56 2035 GMT
        Subject:
            countryName               = BD
            stateOrProvinceName       = Dhaka
            organizationName          = EWU
            organizationalUnitName    = Cyber_Security
            commonName                = Prinom
            emailAddress              = prinom@acmesub_ca.com
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                FE:16:9D:83:98:04:66:81:7C:C1:98:A6:37:DF:3D:DB:C9:F0:01:72
            X509v3 Authority Key Identifier:
                keyid:0D:20:BC:98:5C:9E:97:B1:22:4C:36:6D:1D:12:6C:26:7A:C1:92:1B

            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
Certificate is to be certified until Jan 11 10:04:56 2035 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
root@prinom:~/ca/root-ca# cat index
V       350111100456Z           30F7CF5C522B5AE3ECC631190F31C3B2        unknown      /C=BD/ST=Dhaka/O=EWU/OU=Cyber_Security/CN=Prinom/emailAddress=prinom@acmesub_ca.com
root@prinom:~/ca/root-ca# openssl x509 -noout -text -in ../sub-ca/certs/sub-ca.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            30:f7:cf:5c:52:2b:5a:e3:ec:c6:31:19:0f:31:c3:b2
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = BD, ST = Dhaka, L = Merul, O = EWU, OU = Cyber_Security, CN = Prinom, emailAddress = prinom@acmeroot_ca.com
        Validity
```

Pinging with server



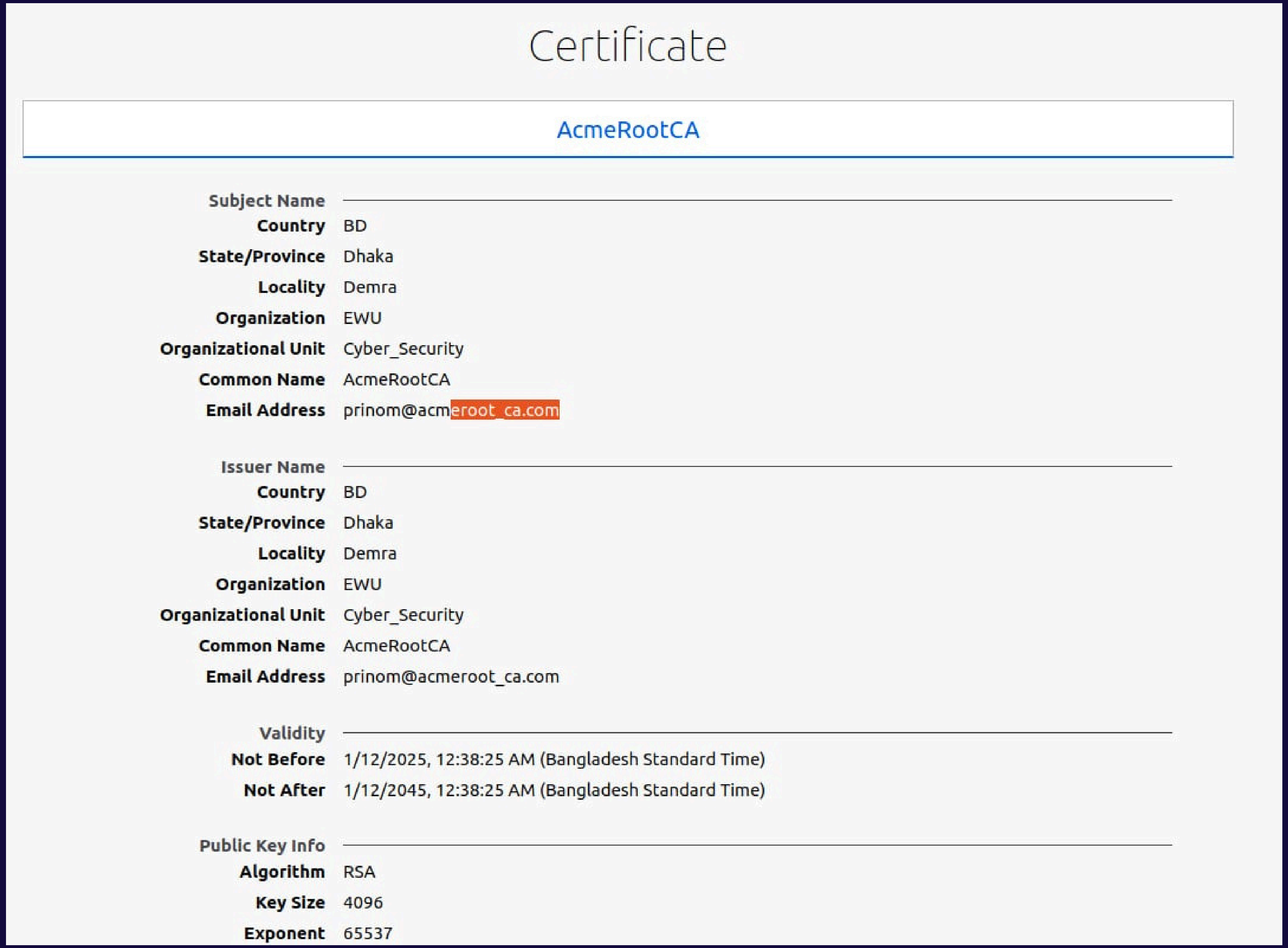
```
root@prinom:~/ca/server# echo "127.0.0.2 www.verysecureserver.com" >> /etc/hosts
root@prinom:~/ca/server# ping www.verysecureserver.com
PING www.verysecureserver.com (127.0.0.2) 56(84) bytes of data.
64 bytes from www.verysecureserver.com (127.0.0.2): icmp_seq=1 ttl=64 time=0.026 ms
64 bytes from www.verysecureserver.com (127.0.0.2): icmp_seq=2 ttl=64 time=0.088 ms
64 bytes from www.verysecureserver.com (127.0.0.2): icmp_seq=3 ttl=64 time=0.053 ms
64 bytes from www.verysecureserver.com (127.0.0.2): icmp_seq=4 ttl=64 time=0.093 ms
64 bytes from www.verysecureserver.com (127.0.0.2): icmp_seq=5 ttl=64 time=0.038 ms
64 bytes from www.verysecureserver.com (127.0.0.2): icmp_seq=6 ttl=64 time=0.096 ms
64 bytes from www.verysecureserver.com (127.0.0.2): icmp_seq=7 ttl=64 time=0.092 ms
64 bytes from www.verysecureserver.com (127.0.0.2): icmp_seq=8 ttl=64 time=0.094 ms
64 bytes from www.verysecureserver.com (127.0.0.2): icmp_seq=9 ttl=64 time=0.094 ms
```

Turning on the ssl port



```
prinom@prinom:~/Desktop$ sudo -i
[sudo] password for prinom:
root@prinom:~# ss -ntl
State   Recv-Q  Send-Q   Local Address:Port   Peer Address:Port Process
LISTEN  0       4096     127.0.0.53%lo:53          0.0.0.0:*
LISTEN  0       5            127.0.0.1:631         0.0.0.0:*
LISTEN  0       5                [::1]:631            [::]:*
root@prinom:~# sudo apt update
Hit:1 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu focal InRelease
Get:3 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease [128 kB]
Hit:4 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Fetched 128 kB in 3s (43.3 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
354 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@prinom:~# sudo apt install curl
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libcurl4
The following NEW packages will be installed:
  curl
The following packages will be upgraded:
  libcurl4
1 upgraded, 1 newly installed, 0 to remove and 353 not upgraded.
Need to get 162 kB/396 kB of archives.
After this operation, 419 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 curl amd64 7.68.0-1ubuntu2.25 [162 kB]
Fetched 162 kB in 2s (77.2 kB/s)
(Reading database ... 179161 files and directories currently installed.)
Preparing to unpack .../libcurl4_7.68.0-1ubuntu2.25_amd64.deb ...
Unpacking libcurl4:amd64 (7.68.0-1ubuntu2.25) over (7.68.0-1ubuntu2.16)
...
Selecting previously unselected package curl.
Preparing to unpack .../curl_7.68.0-1ubuntu2.25_amd64.deb ...
Unpacking curl (7.68.0-1ubuntu2.25) ...
Setting up libcurl4:amd64 (7.68.0-1ubuntu2.25) ...
Setting up curl (7.68.0-1ubuntu2.25) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.9) ...
root@prinom:~# cp ca/root-ca/certs/ca.crt /usr/local/share/ca-certificates/
root@prinom:~# update-ca-certificates -v
/usr/sbin/update-ca-certificates: [--verbose] [--fresh]
root@prinom:~# 
```

Root CA certificate



Certificate

AcmeRootCA

Subject Name

Country	BD
State/Province	Dhaka
Locality	Demra
Organization	EWU
Organizational Unit	Cyber_Security
Common Name	AcmeRootCA
Email Address	prinom@acmeroot_ca.com

Issuer Name

Country	BD
State/Province	Dhaka
Locality	Demra
Organization	EWU
Organizational Unit	Cyber_Security
Common Name	AcmeRootCA
Email Address	prinom@acmeroot_ca.com

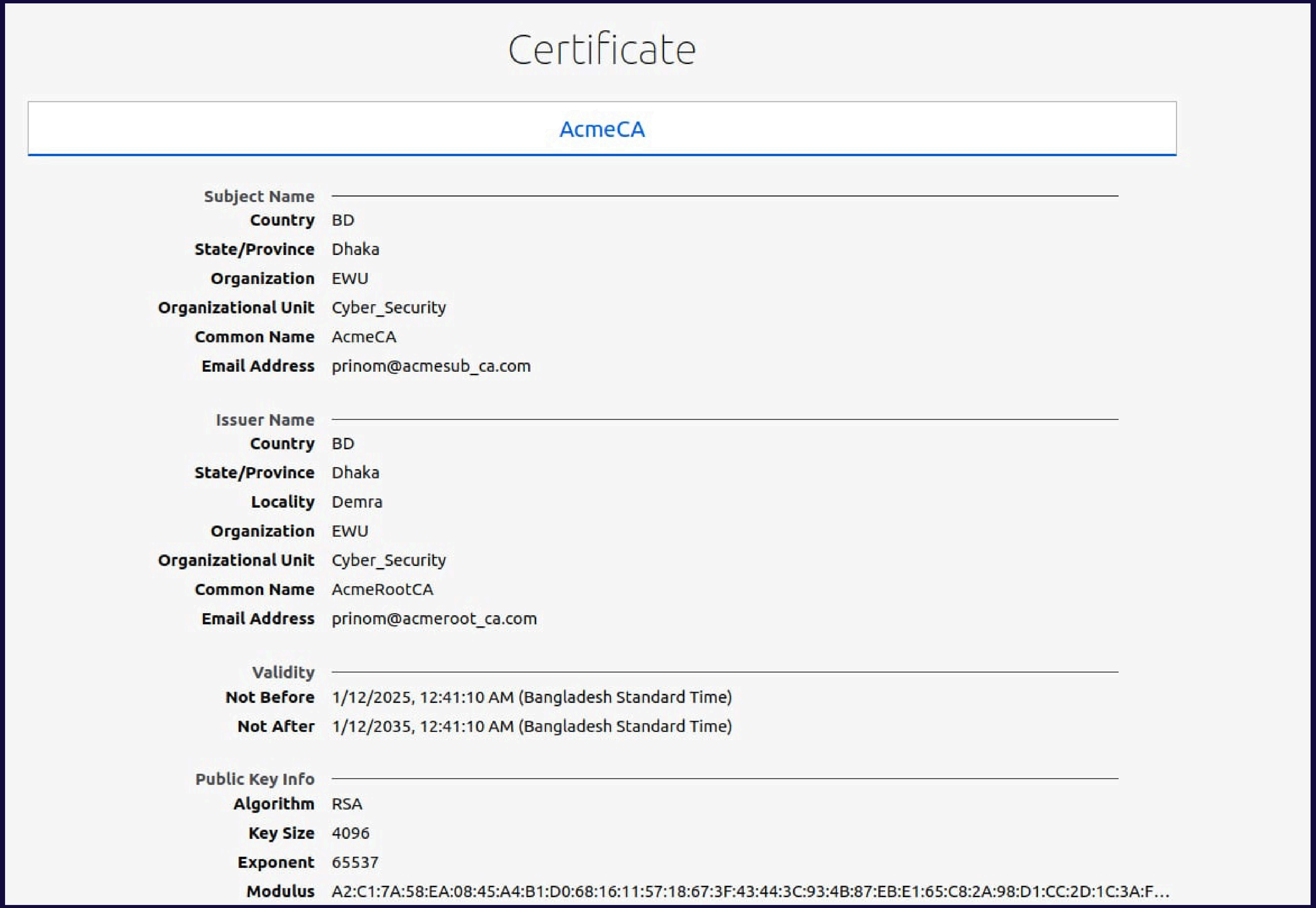
Validity

Not Before	1/12/2025, 12:38:25 AM (Bangladesh Standard Time)
Not After	1/12/2045, 12:38:25 AM (Bangladesh Standard Time)

Public Key Info

Algorithm	RSA
Key Size	4096
Exponent	65537

Sub CA Certificate

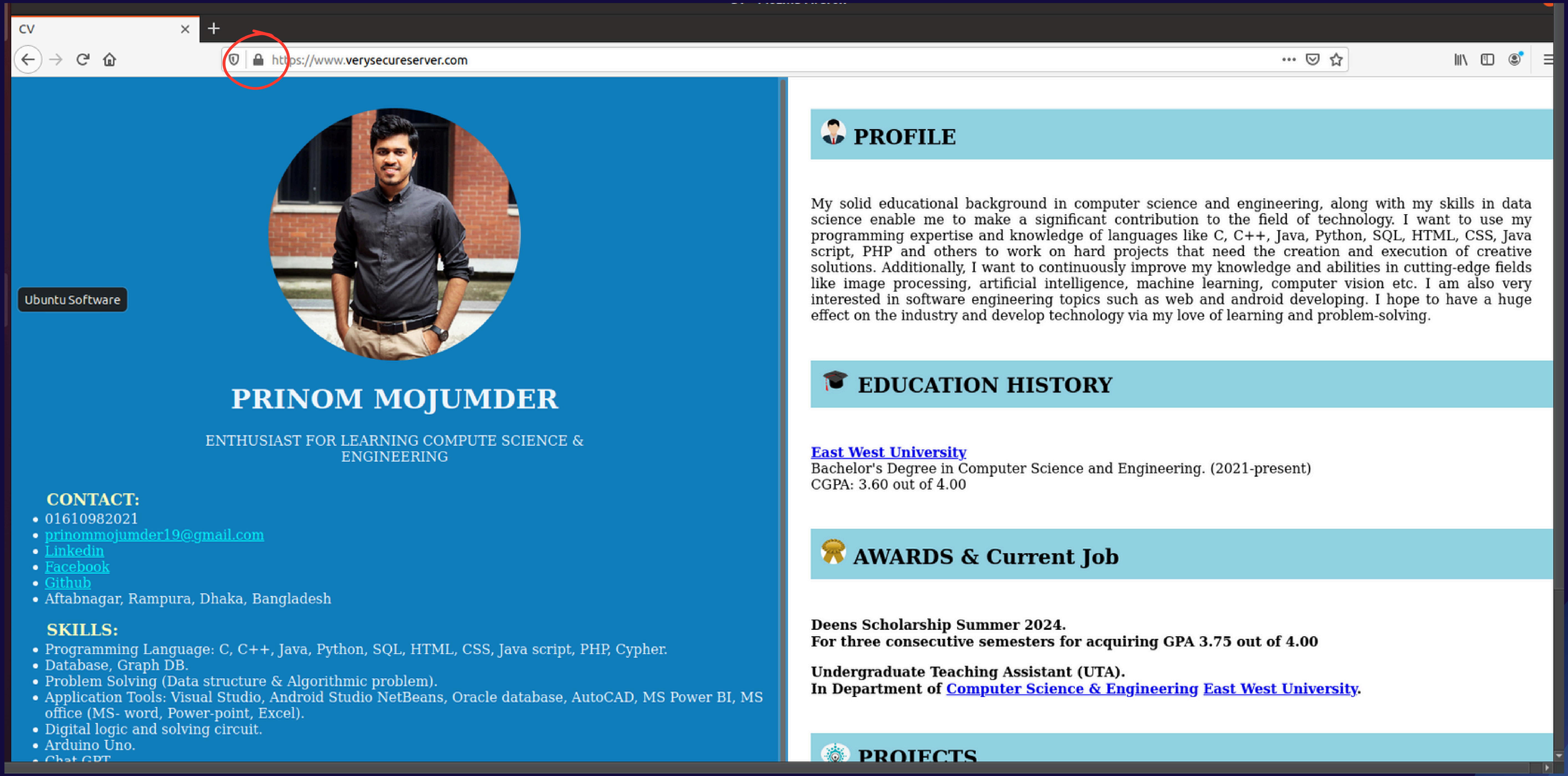


Certificate

AcmeCA

Subject Name	
Country	BD
State/Province	Dhaka
Organization	EWU
Organizational Unit	Cyber_Security
Common Name	AcmeCA
Email Address	prinom@acmesub_ca.com
Issuer Name	
Country	BD
State/Province	Dhaka
Locality	Demra
Organization	EWU
Organizational Unit	Cyber_Security
Common Name	AcmeRootCA
Email Address	prinom@acmeroot_ca.com
Validity	
Not Before	1/12/2025, 12:41:10 AM (Bangladesh Standard Time)
Not After	1/12/2035, 12:41:10 AM (Bangladesh Standard Time)
Public Key Info	
Algorithm	RSA
Key Size	4096
Exponent	65537
Modulus	A2:C1:7A:58:EA:08:45:A4:B1:D0:68:16:11:57:18:67:3F:43:44:3C:93:4B:87:EB:E1:65:C8:2A:98:D1:CC:2D:1C:3A:F…

Web Server



PRINOM MOJUMDER

ENTHUSIAST FOR LEARNING COMPUTE SCIENCE & ENGINEERING

CONTACT:

- 01610982021
- prinommojumder19@gmail.com
- Linkedin
- Facebook
- Github
- Aftabnagar, Rampura, Dhaka, Bangladesh

SKILLS:

- Programming Language: C, C++, Java, Python, SQL, HTML, CSS, Java script, PHP, Cypher.
- Database, Graph DB.
- Problem Solving (Data structure & Algorithmic problem).
- Application Tools: Visual Studio, Android Studio NetBeans, Oracle database, AutoCAD, MS Power BI, MS office (MS- word, Power-point, Excel).
- Digital logic and solving circuit.
- Arduino Uno.
- Chat GPT

PROFILE

My solid educational background in computer science and engineering, along with my skills in data science enable me to make a significant contribution to the field of technology. I want to use my programming expertise and knowledge of languages like C, C++, Java, Python, SQL, HTML, CSS, Java script, PHP and others to work on hard projects that need the creation and execution of creative solutions. Additionally, I want to continuously improve my knowledge and abilities in cutting-edge fields like image processing, artificial intelligence, machine learning, computer vision etc. I am also very interested in software engineering topics such as web and android developing. I hope to have a huge effect on the industry and develop technology via my love of learning and problem-solving.

EDUCATION HISTORY

East West University
Bachelor's Degree in Computer Science and Engineering. (2021-present)
CGPA: 3.60 out of 4.00

AWARDS & Current Job

Deens Scholarship Summer 2024.
For three consecutive semesters for acquiring GPA 3.75 out of 4.00

Undergraduate Teaching Assistant (UTA).
In Department of Computer Science & Engineering East West University.

PROJECTS

This is a secured web server

Page 10

THANK YOU

-