Individual Assignment 6.1: Potential Security Risk Ahead

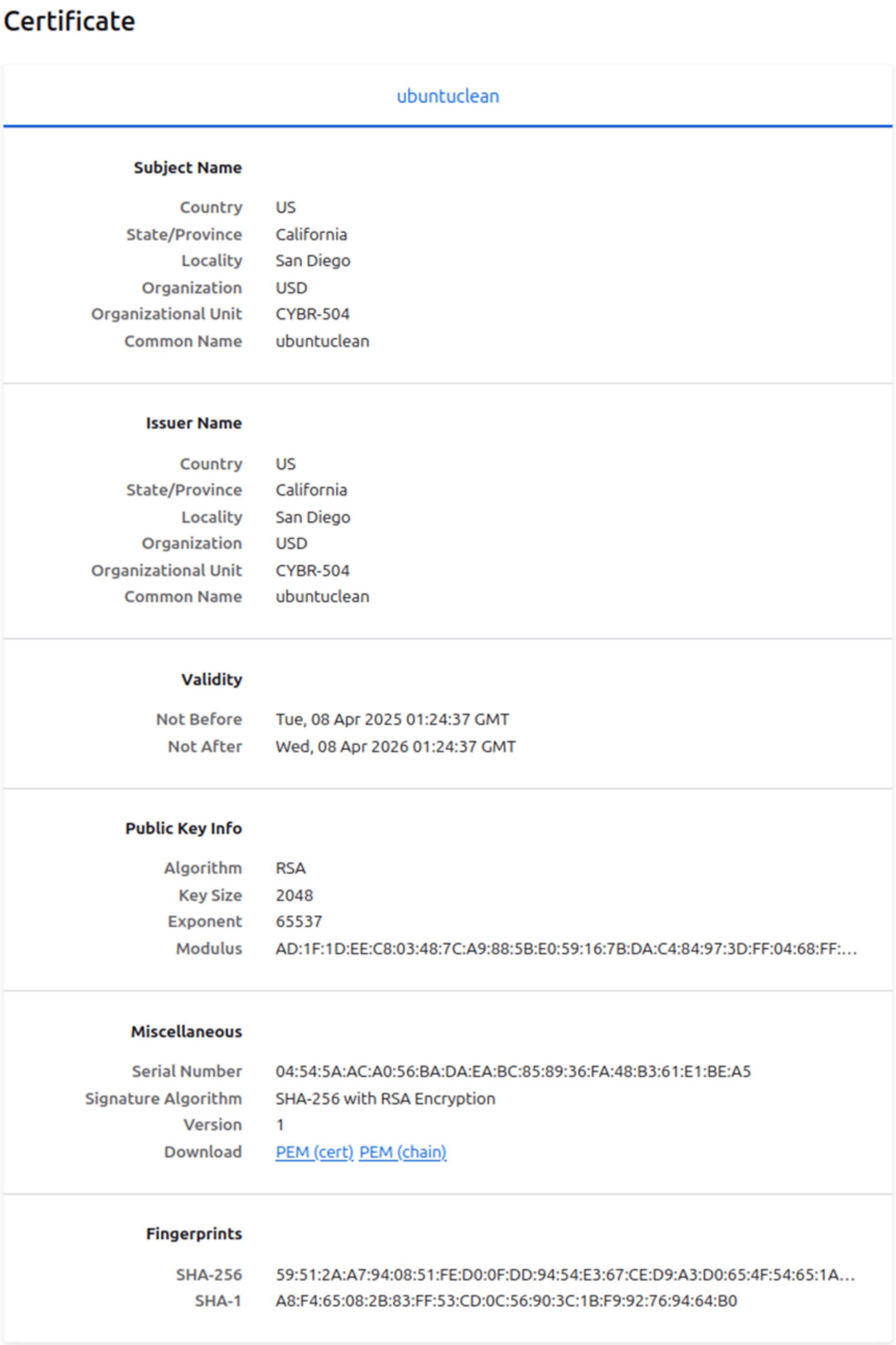
Kayvon Karimi

Cyber-504 Applied Cryptography

Professor Steven Templeton

4/12/2025

Screenshot Deliverables

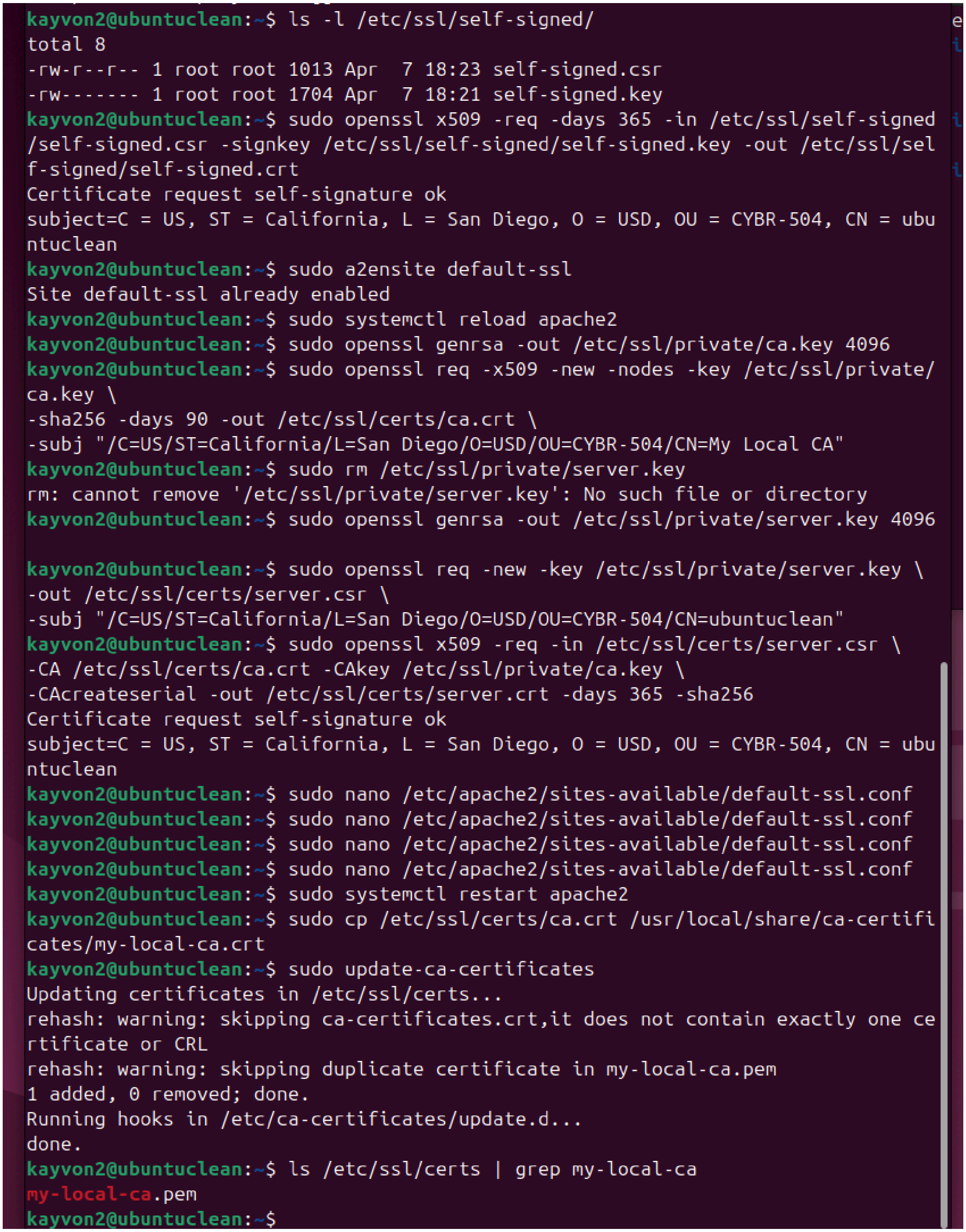


Certificate

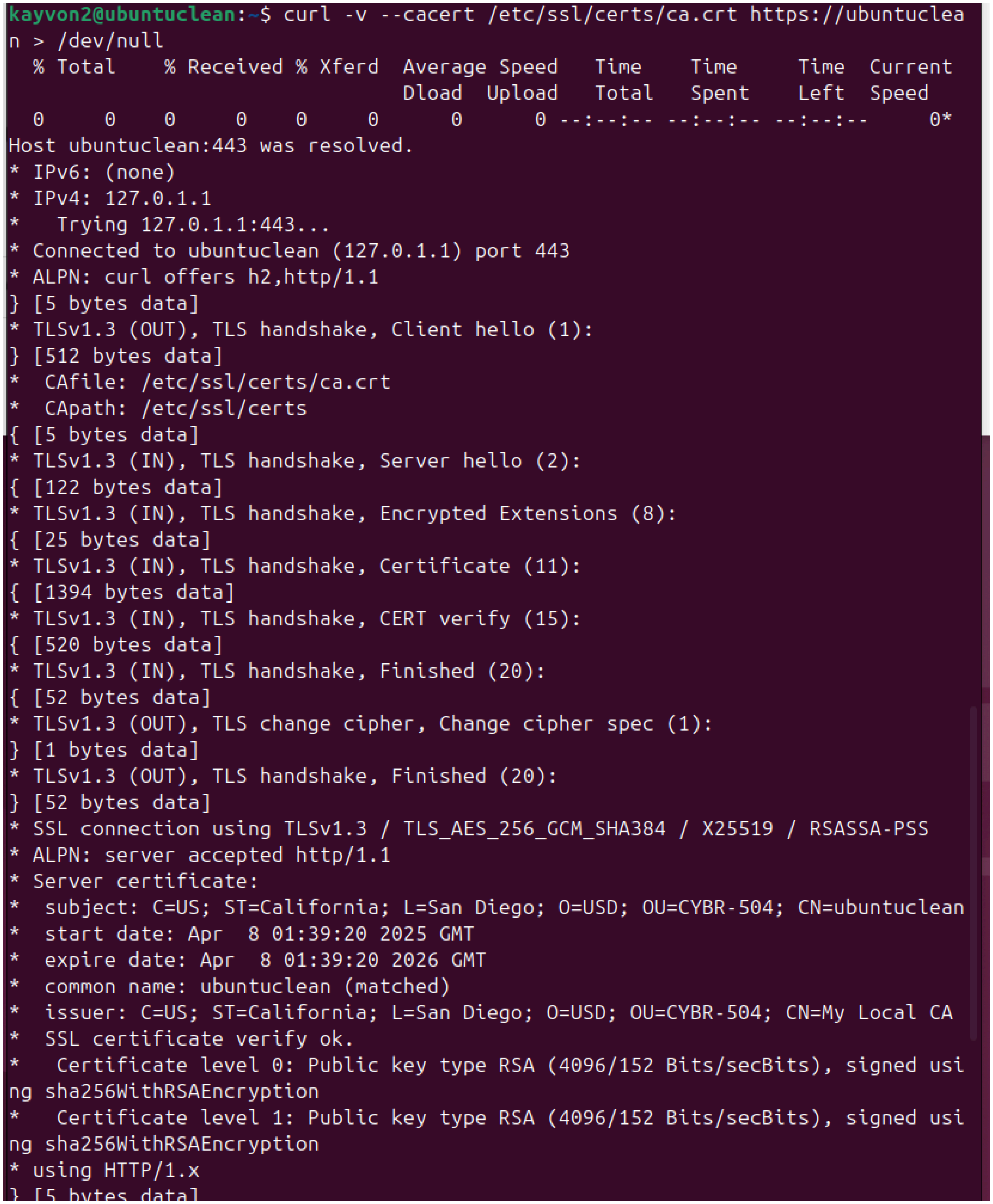
ubuntuclean

Subject Name	
Country	US
State/Province	California
Locality	San Diego
Organization	USD
Organizational Unit	CYBR-504
Common Name	ubuntuclean
Issuer Name	
Country	US
State/Province	California
Locality	San Diego
Organization	USD
Organizational Unit	CYBR-504
Common Name	ubuntuclean
Validity	
Not Before	Tue, 08 Apr 2025 01:24:37 GMT
Not After	Wed, 08 Apr 2026 01:24:37 GMT
Public Key Info	
Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	AD:1F:1D:EE:C8:03:48:7C:A9:88:5B:E0:59:16:7B:DA:C4:84:97:3D:FF:04:68:FF:...
Miscellaneous	
Serial Number	04:54:5A:AC:A0:56:BA:DA:EA:BC:85:89:36:FA:48:B3:61:E1:BE:A5
Signature Algorithm	SHA-256 with RSA Encryption
Version	1
Download	PEM (cert) PEM (chain)
Fingerprints	
SHA-256	59:51:2A:A7:94:08:51:FE:D0:0F:DD:94:54:E3:67:CE:D9:A3:D0:65:4F:54:65:1A...
SHA-1	A8:F4:65:08:2B:83:FF:53:CD:0C:56:90:3C:1B:F9:92:76:94:64:B0

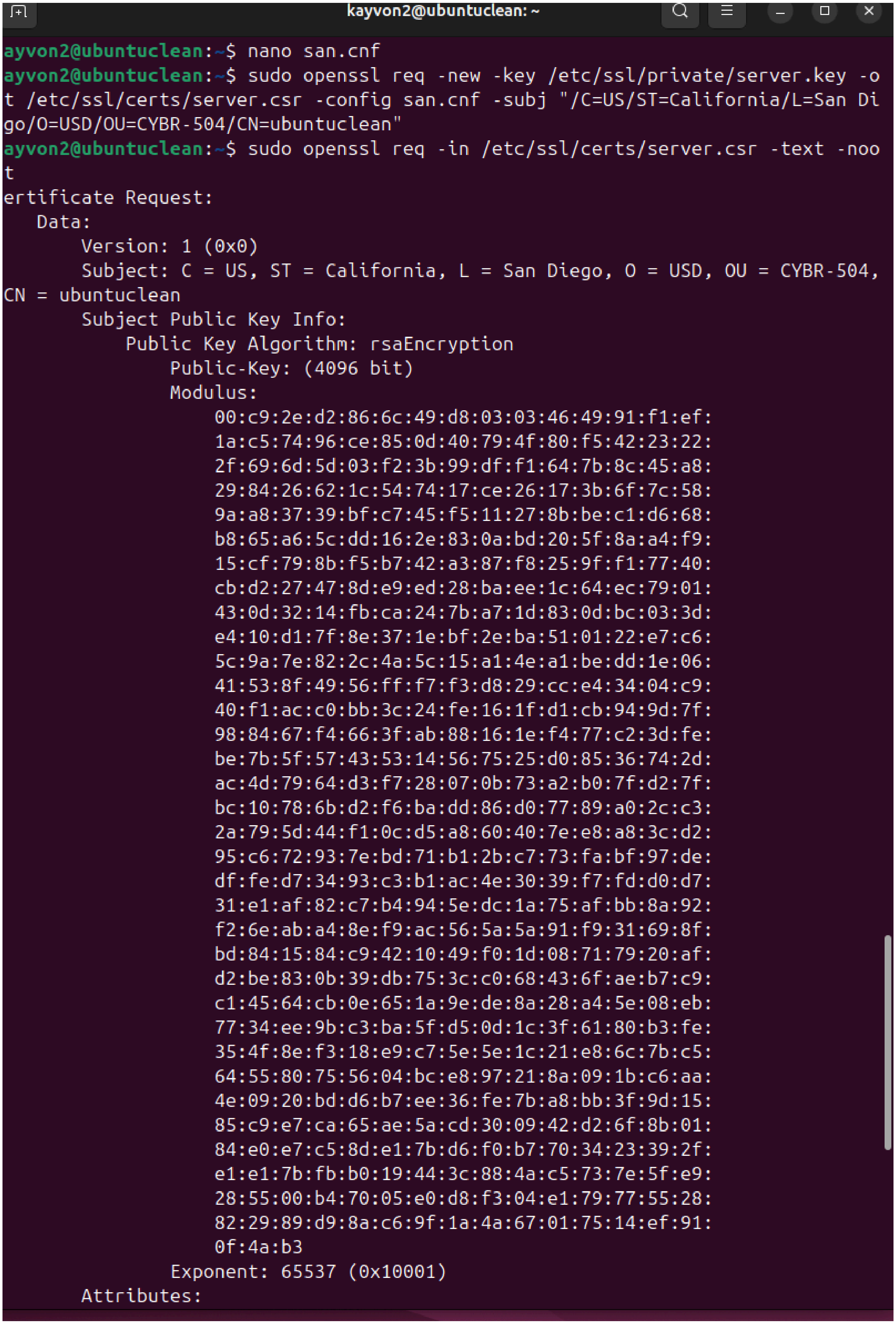
(Initial HTTPS Certificate – Self-Signed (Before CA Signing))



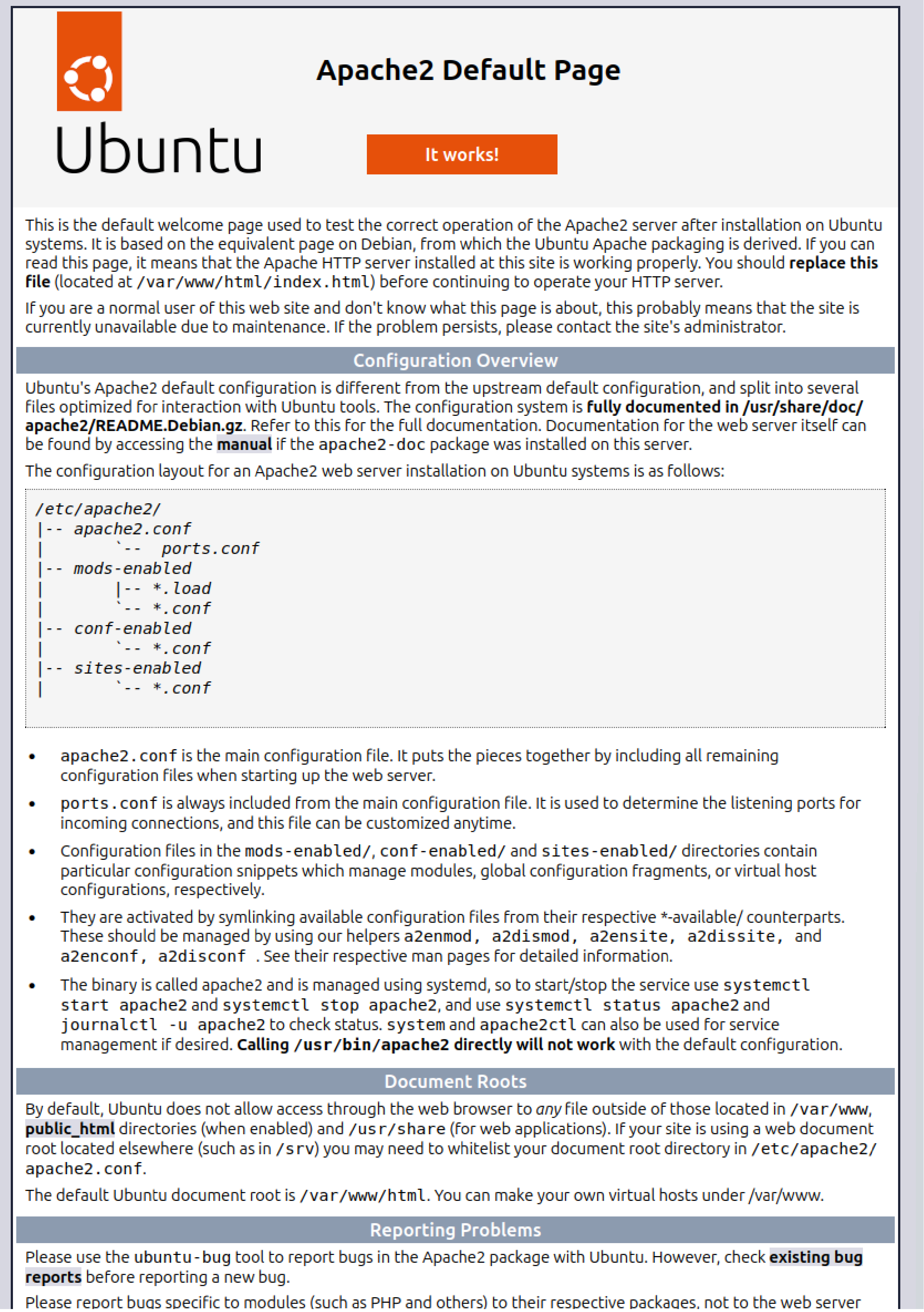
```
kayvon2@ubuntuclean:~$ ls -l /etc/ssl/self-signed/
total 8
-rw-r--r-- 1 root root 1013 Apr  7 18:23 self-signed.csr
-rw------- 1 root root 1704 Apr  7 18:21 self-signed.key
kayvon2@ubuntuclean:~$ sudo openssl x509 -req -days 365 -in /etc/ssl/self-signed
/self-signed.csr -signkey /etc/ssl/self-signed/self-signed.key -out /etc/ssl/sel
f-signed/self-signed.crt
Certificate request self-signature ok
subject=C = US, ST = California, L = San Diego, O = USD, OU = CYBR-504, CN = ubu
ntuclean
kayvon2@ubuntuclean:~$ sudo a2ensite default-ssl
Site default-ssl already enabled
kayvon2@ubuntuclean:~$ sudo systemctl reload apache2
kayvon2@ubuntuclean:~$ sudo openssl genrsa -out /etc/ssl/private/ca.key 4096
kayvon2@ubuntuclean:~$ sudo openssl req -x509 -new -nodes -key /etc/ssl/private/
ca.key \
-sha256 -days 90 -out /etc/ssl/certs/ca.crt \
-subj "/C=US/ST=California/L=San Diego/O=USD/OU=CYBR-504/CN=My Local CA"
kayvon2@ubuntuclean:~$ sudo rm /etc/ssl/private/server.key
rm: cannot remove '/etc/ssl/private/server.key': No such file or directory
kayvon2@ubuntuclean:~$ sudo openssl genrsa -out /etc/ssl/private/server.key 4096

kayvon2@ubuntuclean:~$ sudo openssl req -new -key /etc/ssl/private/server.key \
-out /etc/ssl/certs/server.csr \
-subj "/C=US/ST=California/L=San Diego/O=USD/OU=CYBR-504/CN=ubuntuclean"
kayvon2@ubuntuclean:~$ sudo openssl x509 -req -in /etc/ssl/certs/server.csr \
-CA /etc/ssl/certs/ca.crt -CAkey /etc/ssl/private/ca.key \
-CAcreateserial -out /etc/ssl/certs/server.crt -days 365 -sha256
Certificate request self-signature ok
subject=C = US, ST = California, L = San Diego, O = USD, OU = CYBR-504, CN = ubu
ntuclean
kayvon2@ubuntuclean:~$ sudo nano /etc/apache2/sites-available/default-ssl.conf
kayvon2@ubuntuclean:~$ sudo nano /etc/apache2/sites-available/default-ssl.conf
kayvon2@ubuntuclean:~$ sudo nano /etc/apache2/sites-available/default-ssl.conf
kayvon2@ubuntuclean:~$ sudo nano /etc/apache2/sites-available/default-ssl.conf
kayvon2@ubuntuclean:~$ sudo systemctl restart apache2
kayvon2@ubuntuclean:~$ sudo cp /etc/ssl/certs/ca.crt /usr/local/share/ca-certifi
cates/my-local-ca.crt
kayvon2@ubuntuclean:~$ sudo update-ca-certificates
Updating certificates in /etc/ssl/certs...
rehash: warning: skipping ca-certificates.crt,it does not contain exactly one ce
rtificate or CRL
rehash: warning: skipping duplicate certificate in my-local-ca.pem
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
kayvon2@ubuntuclean:~$ ls /etc/ssl/certs | grep my-local-ca
my-local-ca.pem
kayvon2@ubuntuclean:~$
```



```
kayvon2@ubuntuclean:~$ curl -v --cacert /etc/ssl/certs/ca.crt https://ubuntuclea
n > /dev/null
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0*
Host ubuntuclean:443 was resolved.
* IPv6: (none)
* IPv4: 127.0.1.1
*   Trying 127.0.1.1:443...
* Connected to ubuntuclean (127.0.1.1) port 443
* ALPN: curl offers h2,http/1.1
} [5 bytes data]
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
} [512 bytes data]
*  CAfile: /etc/ssl/certs/ca.crt
*  CApath: /etc/ssl/certs
{ [5 bytes data]
* TLSv1.3 (IN), TLS handshake, Server hello (2):
{ [122 bytes data]
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
{ [25 bytes data]
* TLSv1.3 (IN), TLS handshake, Certificate (11):
{ [1394 bytes data]
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
{ [520 bytes data]
* TLSv1.3 (IN), TLS handshake, Finished (20):
{ [52 bytes data]
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
} [1 bytes data]
* TLSv1.3 (OUT), TLS handshake, Finished (20):
} [52 bytes data]
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384 / X25519 / RSASSA-PSS
* ALPN: server accepted http/1.1
* Server certificate:
*  subject: C=US; ST=California; L=San Diego; O=USD; OU=CYBR-504; CN=ubuntuclean
*  start date: Apr  8 01:39:20 2025 GMT
*  expire date: Apr  8 01:39:20 2026 GMT
*  common name: ubuntuclean (matched)
*  issuer: C=US; ST=California; L=San Diego; O=USD; OU=CYBR-504; CN=My Local CA
*  SSL certificate verify ok.
*   Certificate level 0: Public key type RSA (4096/152 Bits/secBits), signed usi
ng sha256WithRSAEncryption
*   Certificate level 1: Public key type RSA (4096/152 Bits/secBits), signed usi
ng sha256WithRSAEncryption
* using HTTP/1.x
} [5 bytes data]
```



```
ayvon2@ubuntuclean:~$ nano san.cnf
ayvon2@ubuntuclean:~$ sudo openssl req -new -key /etc/ssl/private/server.key -o
t /etc/ssl/certs/server.csr -config san.cnf -subj "/C=US/ST=California/L=San Di
go/O=USD/OU=CYBR-504/CN=ubuntuclean"
ayvon2@ubuntuclean:~$ sudo openssl req -in /etc/ssl/certs/server.csr -text -noo
t
ertificate Request:
   Data:
       Version: 1 (0x0)
       Subject: C = US, ST = California, L = San Diego, O = USD, OU = CYBR-504,
CN = ubuntuclean
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
               Public-Key: (4096 bit)
               Modulus:
                   00:c9:2e:d2:86:6c:49:d8:03:03:46:49:91:f1:ef:
                   1a:c5:74:96:ce:85:0d:40:79:4f:80:f5:42:23:22:
                   2f:69:6d:5d:03:f2:3b:99:df:f1:64:7b:8c:45:a8:
                   29:84:26:62:1c:54:74:17:ce:26:17:3b:6f:7c:58:
                   9a:a8:37:39:bf:c7:45:f5:11:27:8b:be:c1:d6:68:
                   b8:65:a6:5c:dd:16:2e:83:0a:bd:20:5f:8a:a4:f9:
                   15:cf:79:8b:f5:b7:42:a3:87:f8:25:9f:f1:77:40:
                   cb:d2:27:47:8d:e9:ed:28:ba:ee:1c:64:ec:79:01:
                   43:0d:32:14:fb:ca:24:7b:a7:1d:83:0d:bc:03:3d:
                   e4:10:d1:7f:8e:37:1e:bf:2e:ba:51:01:22:e7:c6:
                   5c:9a:7e:82:2c:4a:5c:15:a1:4e:a1:be:dd:1e:06:
                   41:53:8f:49:56:ff:f7:f3:d8:29:cc:e4:34:04:c9:
                   40:f1:ac:c0:bb:3c:24:fe:16:1f:d1:cb:94:9d:7f:
                   98:84:67:f4:66:3f:ab:88:16:1e:f4:77:c2:3d:fe:
                   be:7b:5f:57:43:53:14:56:75:25:d0:85:36:74:2d:
                   ac:4d:79:64:d3:f7:28:07:0b:73:a2:b0:7f:d2:7f:
                   bc:10:78:6b:d2:f6:ba:dd:86:d0:77:89:a0:2c:c3:
                   2a:79:5d:44:f1:0c:d5:a8:60:40:7e:e8:a8:3c:d2:
                   95:c6:72:93:7e:bd:71:b1:2b:c7:73:fa:bf:97:de:
                   df:fe:d7:34:93:c3:b1:ac:4e:30:39:f7:fd:d0:d7:
                   31:e1:af:82:c7:b4:94:5e:dc:1a:75:af:bb:8a:92:
                   f2:6e:ab:a4:8e:f9:ac:56:5a:5a:91:f9:31:69:8f:
                   bd:84:15:84:c9:42:10:49:f0:1d:08:71:79:20:af:
                   d2:be:83:0b:39:db:75:3c:c0:68:43:6f:ae:b7:c9:
                   c1:45:64:cb:0e:65:1a:9e:de:8a:28:a4:5e:08:eb:
                   77:34:ee:9b:c3:ba:5f:d5:0d:1c:3f:61:80:b3:fe:
                   35:4f:8e:f3:18:e9:c7:5e:5e:1c:21:e8:6c:7b:c5:
                   64:55:80:75:56:04:bc:e8:97:21:8a:09:1b:c6:aa:
                   4e:09:20:bd:d6:b7:ee:36:fe:7b:a8:bb:3f:9d:15:
                   85:c9:e7:ca:65:ae:5a:cd:30:09:42:d2:6f:8b:01:
                   84:e0:e7:c5:8d:e1:7b:d6:f0:b7:70:34:23:39:2f:
                   e1:e1:7b:fb:b0:19:44:3c:88:4a:c5:73:7e:5f:e9:
                   28:55:00:b4:70:05:e0:d8:f3:04:e1:79:77:55:28:
                   82:29:89:d9:8a:c6:9f:1a:4a:67:01:75:14:ef:91:
                   0f:4a:b3
               Exponent: 65537 (0x10001)
       Attributes:
```



Ubuntu

Apache2 Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers `a2enmod, a2dismod, a2ensite, a2dissite,` and `a2enconf, a2disconf` . See their respective man pages for detailed information.
- The binary is called apache2 and is managed using systemd, so to start/stop the service use `systemctl start apache2` and `systemctl stop apache2`, and use `systemctl status apache2` and `journalctl -u apache2` to check status. `system` and `apache2ctl` can also be used for service management if desired. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

Document Roots

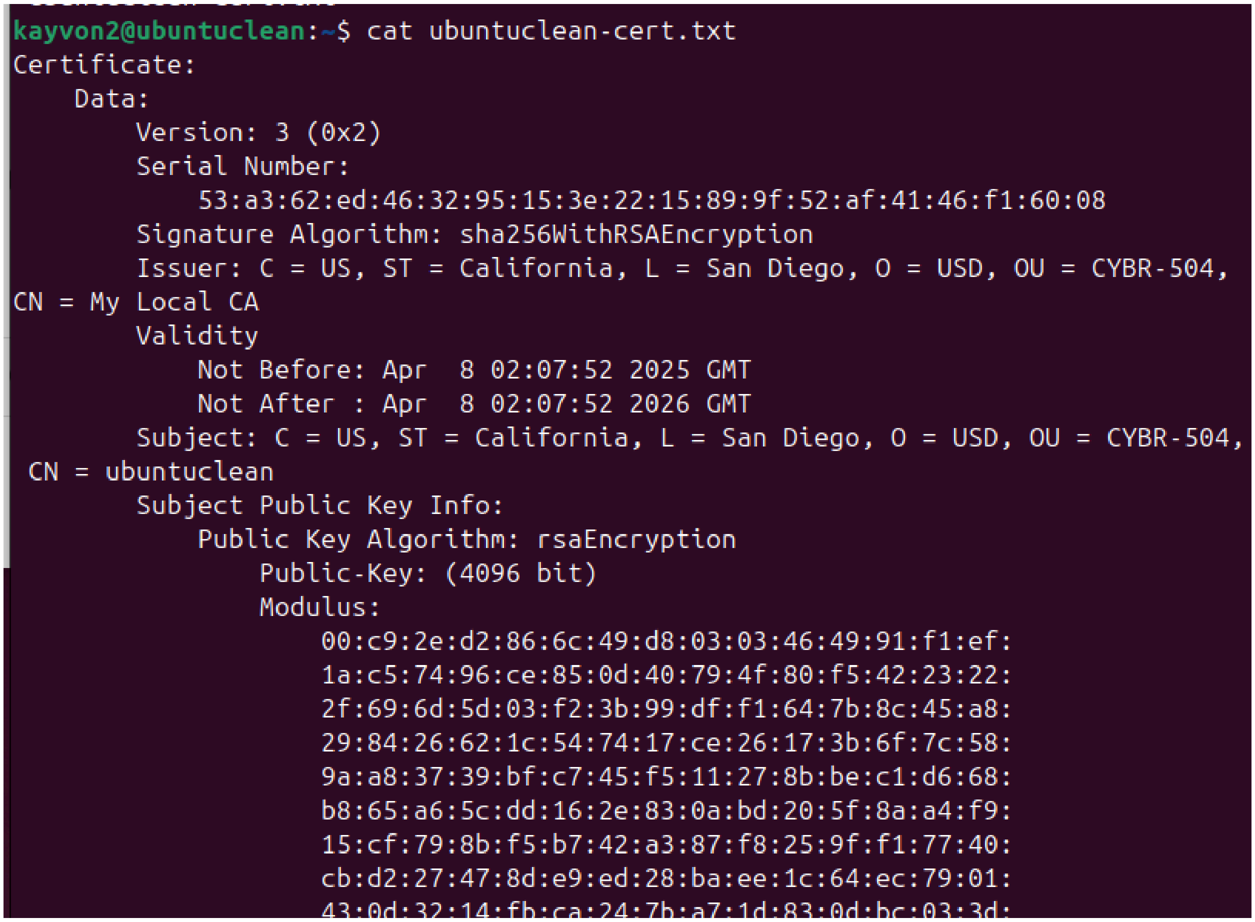
By default, Ubuntu does not allow access through the web browser to *any* file outside of those located in `/var/www`, **public_html** directories (when enabled) and `/usr/share` (for web applications). If your site is using a web document root located elsewhere (such as in `/srv`) you may need to whitelist your document root directory in `/etc/apache2/apache2.conf`.

The default Ubuntu document root is `/var/www/html`. You can make your own virtual hosts under /var/www.

Reporting Problems

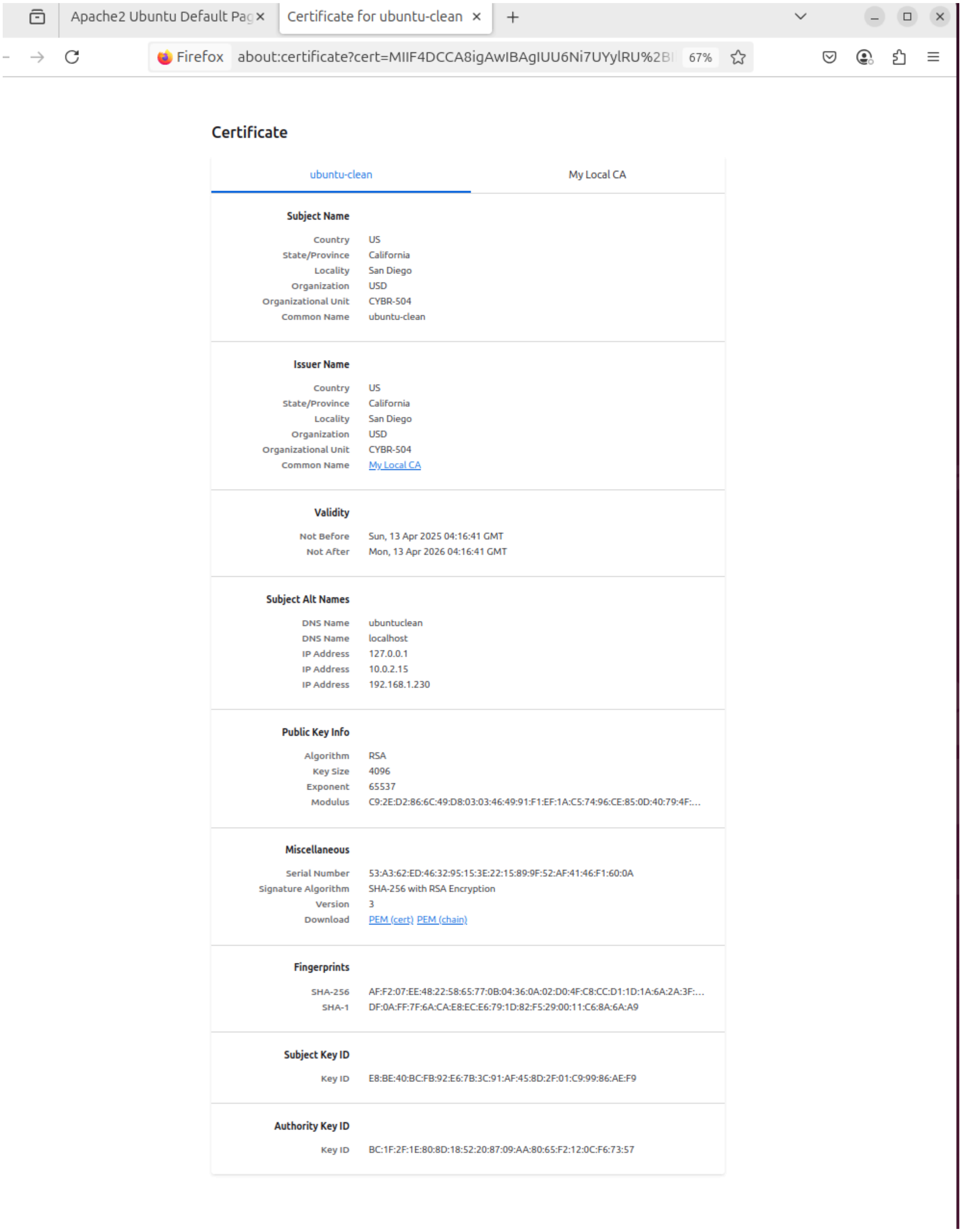
Please use the `ubuntu-bug` tool to report bugs in the Apache2 package with Ubuntu. However, check **existing bug reports** before reporting a new bug.

Please report bugs specific to modules (such as PHP and others) to their respective packages, not to the web server



```
kayvon2@ubuntuclean:~$ cat ubuntuclean-cert.txt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            53:a3:62:ed:46:32:95:15:3e:22:15:89:9f:52:af:41:46:f1:60:08
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = California, L = San Diego, O = USD, OU = CYBR-504,
CN = My Local CA
        Validity
            Not Before: Apr  8 02:07:52 2025 GMT
            Not After : Apr  8 02:07:52 2026 GMT
        Subject: C = US, ST = California, L = San Diego, O = USD, OU = CYBR-504,
 CN = ubuntuclean
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:c9:2e:d2:86:6c:49:d8:03:03:46:49:91:f1:ef:
                    1a:c5:74:96:ce:85:0d:40:79:4f:80:f5:42:23:22:
                    2f:69:6d:5d:03:f2:3b:99:df:f1:64:7b:8c:45:a8:
                    29:84:26:62:1c:54:74:17:ce:26:17:3b:6f:7c:58:
                    9a:a8:37:39:bf:c7:45:f5:11:27:8b:be:c1:d6:68:
                    b8:65:a6:5c:dd:16:2e:83:0a:bd:20:5f:8a:a4:f9:
                    15:cf:79:8b:f5:b7:42:a3:87:f8:25:9f:f1:77:40:
                    cb:d2:27:47:8d:e9:ed:28:ba:ee:1c:64:ec:79:01:
                    43:0d:32:14:fb:ca:24:7b:a7:1d:83:0d:bc:03:3d:
```

Browser Verification of CA-Signed Certificate on Ubuntu Firefox Browser


Apache2 Ubuntu Default Pag
Certificate for ubuntu-clean
Firefox
about:certificate?cert=MIIF4DCCA8igAwIBAgIUU6Ni7UYylRU%2B
67%

Certificate

ubuntu-clean | My Local CA

Subject Name

Country	US
State/Province	California
Locality	San Diego
Organization	USD
Organizational Unit	CYBR-504
Common Name	ubuntu-clean

Issuer Name

Country	US
State/Province	California
Locality	San Diego
Organization	USD
Organizational Unit	CYBR-504
Common Name	My Local CA

Validity

Not Before	Sun, 13 Apr 2025 04:16:41 GMT
Not After	Mon, 13 Apr 2026 04:16:41 GMT

Subject Alt Names

DNS Name	ubuntuclean
DNS Name	localhost
IP Address	127.0.0.1
IP Address	10.0.2.15
IP Address	192.168.1.230

Public Key Info

Algorithm	RSA
Key Size	4096
Exponent	65537
Modulus	C9:2E:D2:86:6C:49:D8:03:03:46:49:91:F1:EF:1A:C5:74:96:CE:85:0D:40:79:4F:...

Miscellaneous

Serial Number	53:A3:62:ED:46:32:95:15:3E:22:15:89:9F:52:AF:41:46:F1:60:0A
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Fingerprints

SHA-256	AF:F2:07:EE:48:22:58:65:77:0B:04:36:0A:02:D0:4F:C8:CC:D1:1D:1A:6A:2A:3F:...
SHA-1	DF:0A:FF:7F:6A:CA:E8:EC:E6:79:1D:82:F5:29:00:11:C6:8A:6A:A9

Subject Key ID

Key ID	E8:BE:40:BC:FB:92:E6:7B:3C:91:AF:45:8D:2F:01:C9:99:86:AE:F9

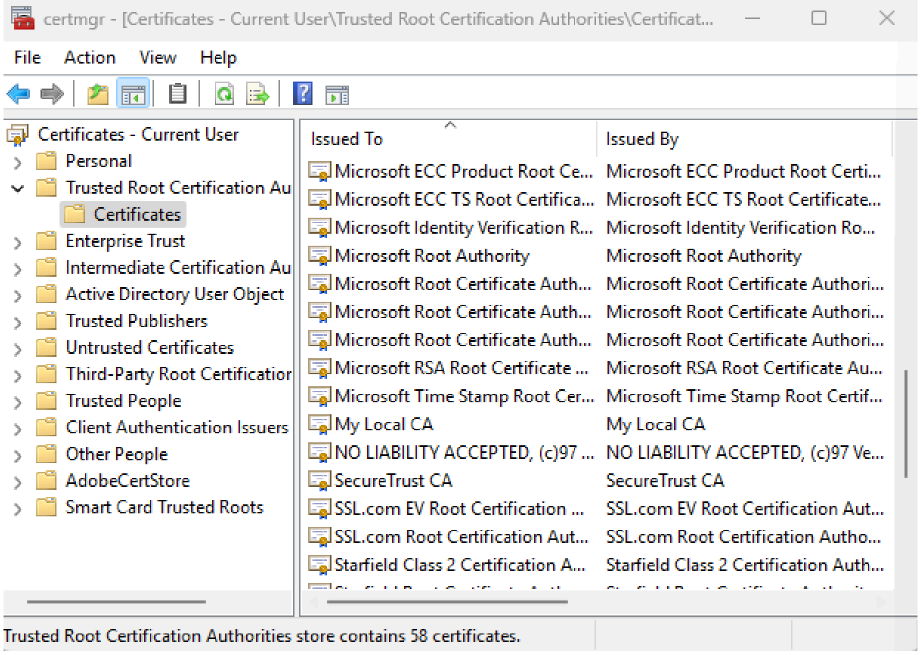
Authority Key ID

Key ID	BC:1F:2F:1E:80:8D:18:52:20:87:09:AA:80:65:F2:12:0C:F6:73:57

EXTRA CREDIT: Installing CA on Windows

To complete the extra credit, I switched my Ubuntu virtual machine from NAT to Bridged mode so that it would receive a LAN IP address (192.168.1.230) that could be accessed from my Windows machine. After doing so, I edited my san.cnf file to include that IP address in the Subject Alternative Name (SAN) section of the certificate configuration. I then regenerated and re-signed the server certificate using my local Certificate Authority. Once restarted, the Apache server on Ubuntu served the updated certificate, and Firefox on Windows recognized it as valid and signed by "My Local CA," displaying a secure HTTPS connection without any warnings.

(Importing the CA on a Windows system)

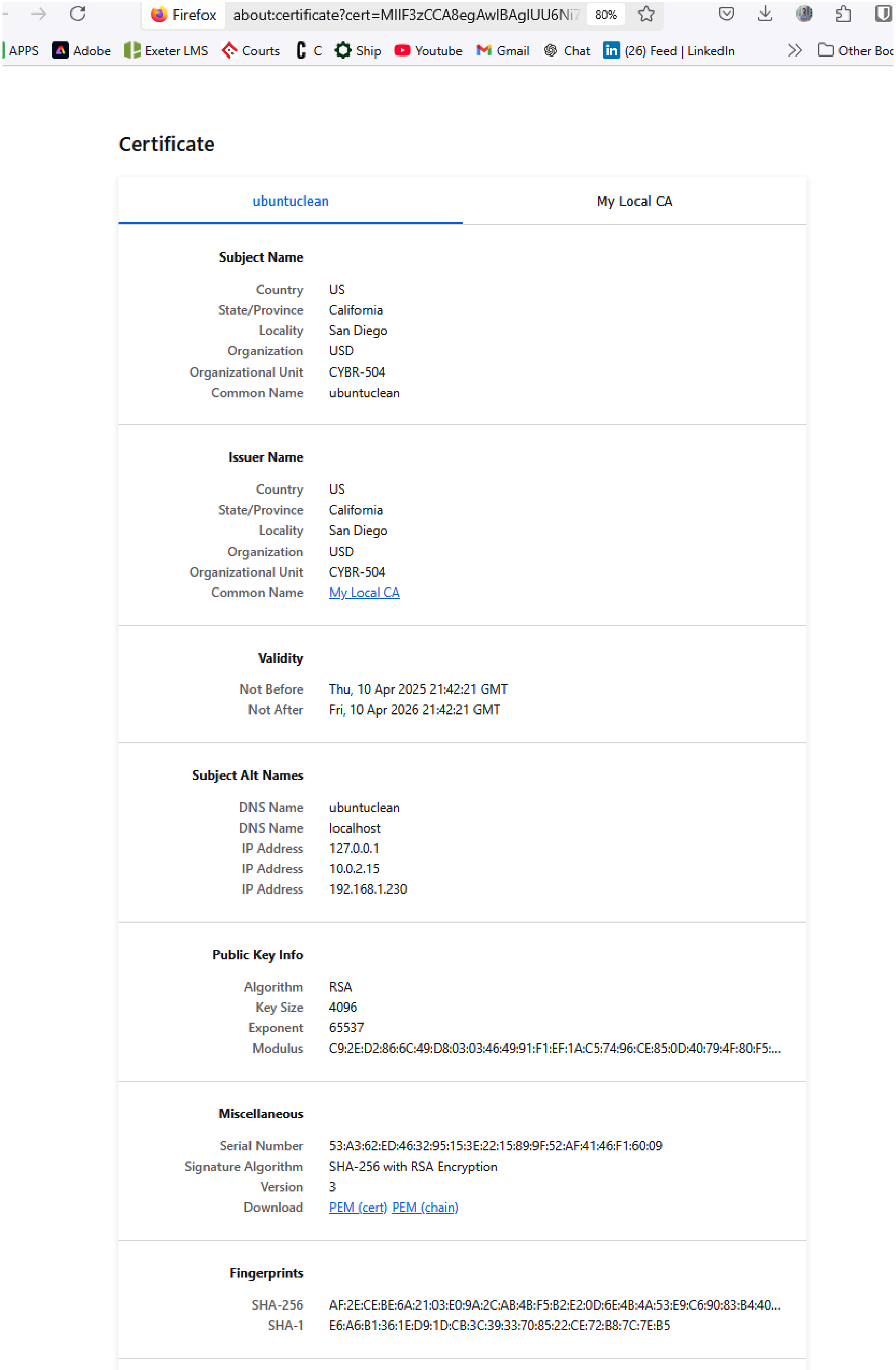

certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificat...
File
Action
View
Help
Certificates - Current User
Personal
Trusted Root Certification Au
Certificates
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Client Authentication Issuers
Other People
AdobeCertStore
Smart Card Trusted Roots

Issued To	Issued By
Microsoft ECC Product Root Ce...	Microsoft ECC Product Root Certi...
Microsoft ECC TS Root Certifica...	Microsoft ECC TS Root Certificate...
Microsoft Identity Verification R...	Microsoft Identity Verification Ro...
Microsoft Root Authority	Microsoft Root Authority
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...
Microsoft RSA Root Certificate ...	Microsoft RSA Root Certificate Au...
Microsoft Time Stamp Root Cer...	Microsoft Time Stamp Root Certif...
My Local CA	My Local CA
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 Ve...
SecureTrust CA	SecureTrust CA
SSL.com EV Root Certification ...	SSL.com EV Root Certification Aut...
SSL.com Root Certification Aut...	SSL.com Root Certification Autho...
Starfield Class 2 Certification A...	Starfield Class 2 Certification Auth...

Trusted Root Certification Authorities store contains 58 certificates.

(Windows Firefox Browser)

(Windows Firefox Browser with My Local CA)



Certificate

ubuntuclean | My Local CA

Subject Name

Country	US
State/Province	California
Locality	San Diego
Organization	USD
Organizational Unit	CYBR-504
Common Name	ubuntuclean

Issuer Name

Country	US
State/Province	California
Locality	San Diego
Organization	USD
Organizational Unit	CYBR-504
Common Name	My Local CA

Validity

Not Before	Thu, 10 Apr 2025 21:42:21 GMT
Not After	Fri, 10 Apr 2026 21:42:21 GMT

Subject Alt Names

DNS Name	ubuntuclean
DNS Name	localhost
IP Address	127.0.0.1
IP Address	10.0.2.15
IP Address	192.168.1.230

Public Key Info

Algorithm	RSA
Key Size	4096
Exponent	65537
Modulus	C9:2E:D2:86:6C:49:D8:03:03:46:49:91:F1:EF:1A:C5:74:96:CE:85:0D:40:79:4F:80:F5:...

Miscellaneous

Serial Number	53:A3:62:ED:46:32:95:15:3E:22:15:89:9F:52:AF:41:46:F1:60:09
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Fingerprints

SHA-256	AF:2E:CE:BE:6A:21:03:E0:9A:2C:AB:4B:F5:B2:E2:0D:6E:4B:4A:53:E9:C6:90:83:B4:40...
SHA-1	E6:A6:B1:36:1E:D9:1D:CB:3C:39:33:70:85:22:CE:72:B8:7C:7E:B5

(Screenshot of text output of CA-signed certificate, also included in submission as PDF)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            53:a3:62:ed:46:32:95:15:3e:22:15:89:9f:52:af:41:46:f1:60:09
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = California, L = San Diego, O = USD, OU = CYBR-504, CN =
My Local CA
        Validity
            Not Before: Apr 10 21:42:21 2025 GMT
            Not After : Apr 10 21:42:21 2026 GMT
        Subject: C = US, ST = California, L = San Diego, O = USD, OU = CYBR-504, CN
= ubuntuclean
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:c9:2e:d2:86:6c:49:d8:03:03:46:49:91:f1:ef:
                    1a:c5:74:96:ce:85:0d:40:79:4f:80:f5:42:23:22:
                    2f:69:6d:5d:03:f2:3b:99:df:f1:64:7b:8c:45:a8:
                    29:84:26:62:1c:54:74:17:ce:26:17:3b:6f:7c:58:
                    9a:a8:37:39:bf:c7:45:f5:11:27:8b:be:c1:d6:68:
                    b8:65:a6:5c:dd:16:2e:83:0a:bd:20:5f:8a:a4:f9:
                    15:cf:79:8b:f5:b7:42:a3:87:f8:25:9f:f1:77:40:
                    cb:d2:27:47:8d:e9:ed:28:ba:ee:1c:64:ec:79:01:
                    43:0d:32:14:fb:ca:24:7b:a7:1d:83:0d:bc:03:3d:
                    e4:10:d1:7f:8e:37:1e:bf:2e:ba:51:01:22:e7:c6:
                    5c:9a:7e:82:2c:4a:5c:15:a1:4e:a1:be:dd:1e:06:
                    41:53:8f:49:56:ff:f7:f3:d8:29:cc:e4:34:04:c9:
                    40:f1:ac:c0:bb:3c:24:fe:16:1f:d1:cb:94:9d:7f:
                    98:84:67:f4:66:3f:ab:88:16:1e:f4:77:c2:3d:fe:
                    be:7b:5f:57:43:53:14:56:75:25:d0:85:36:74:2d:
                    ac:4d:79:64:d3:f7:28:07:0b:73:a2:b0:7f:d2:7f:
                    bc:10:78:6b:d2:f6:ba:dd:86:d0:77:89:a0:2c:c3:
                    2a:79:5d:44:f1:0c:d5:a8:60:40:7e:e8:a8:3c:d2:
                    95:c6:72:93:7e:bd:71:b1:2b:c7:73:fa:bf:97:de:
                    df:fe:d7:34:93:c3:b1:ac:4e:30:39:f7:fd:d0:d7:
                    31:e1:af:82:c7:b4:94:5e:dc:1a:75:af:bb:8a:92:
                    f2:6e:ab:a4:8e:f9:ac:56:5a:5a:91:f9:31:69:8f:
                    bd:84:15:84:c9:42:10:49:f0:1d:08:71:79:20:af:
                    d2:be:83:0b:39:db:75:3c:c0:68:43:6f:ae:b7:c9:
                    c1:45:64:cb:0e:65:1a:9e:de:8a:28:a4:5e:08:eb:
                    77:34:ee:9b:c3:ba:5f:d5:0d:1c:3f:61:80:b3:fe:
                    35:4f:8e:f3:18:e9:c7:5e:5e:1c:21:e8:6c:7b:c5:
                    64:55:80:75:56:04:bc:e8:97:21:8a:09:1b:c6:aa:
                    4e:09:20:bd:d6:b7:ee:36:fe:7b:a8:bb:3f:9d:15:
                    85:c9:e7:ca:65:ae:5a:cd:30:09:42:d2:6f:8b:01:
                    84:e0:e7:c5:8d:e1:7b:d6:f0:b7:70:34:23:39:2f:
                    e1:e1:7b:fb:b0:19:44:3c:88:4a:c5:73:7e:5f:e9:
                    28:55:00:b4:70:05:e0:d8:f3:04:e1:79:77:55:28:
```

```
                    82:29:89:d9:8a:c6:9f:1a:4a:67:01:75:14:ef:91:
                    0f:4a:b3
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:ubuntuclean, DNS:localhost, IP Address:127.0.0.1, IP
Address:10.0.2.15, IP Address:192.168.1.230
            X509v3 Subject Key Identifier:
                E8:BE:40:BC:FB:92:E6:7B:3C:91:AF:45:8D:2F:01:C9:99:86:AE:F9
            X509v3 Authority Key Identifier:
                BC:1F:2F:1E:80:8D:18:52:20:87:09:AA:80:65:F2:12:0C:F6:73:57
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        6c:cb:5c:1c:d1:84:0d:14:56:68:12:65:d4:12:0e:46:1f:0f:
        57:80:c9:21:aa:20:0a:cc:15:a8:b7:e1:ce:31:d2:69:28:eb:
        c8:76:66:a7:49:3a:45:dc:2a:a4:cd:3f:a4:0f:f9:04:54:05:
        f4:cf:32:2d:02:c8:3b:f6:06:3d:23:2d:9a:67:6f:51:d3:d1:
        d8:a6:e9:6b:18:25:e2:aa:30:c8:e0:a5:67:67:fe:96:22:03:
        ef:cc:a5:08:15:6f:3f:74:e6:9d:7f:c2:ec:8e:77:4e:6d:52:
        5e:c7:8c:42:ae:43:46:58:8c:06:4c:f5:4c:ad:3e:0f:25:7d:
        93:77:8c:9a:a4:9c:14:4b:51:3b:dd:9a:49:e4:7b:76:29:4c:
        ed:f9:c8:68:0d:53:eb:e4:23:17:7d:a5:7e:6d:1d:43:31:12:
        37:0f:4b:61:30:09:17:cd:e6:9f:e4:cb:71:a3:a2:50:90:ed:
        75:46:79:1e:05:a9:a6:74:9b:98:89:2b:c4:c5:be:68:94:c7:
        64:83:d4:27:38:7e:1f:48:fb:41:79:f3:53:d7:38:f2:13:80:
        02:a4:b0:1d:79:60:0f:27:56:3b:7f:56:49:05:3e:bf:e2:bc:
        49:e1:c1:f2:38:16:eb:82:81:0b:76:1b:68:71:33:0e:34:02:
        18:c9:a7:28:3b:a9:38:84:2f:f9:46:4b:ba:6c:53:d1:e0:f8:
        71:f4:64:94:29:f5:25:07:00:8a:d0:11:f0:d7:2a:c8:08:fe:
        99:cb:a6:00:6f:d2:3d:04:e3:b2:79:6f:0a:b4:7b:49:7b:e1:
        3c:ef:56:f8:7e:36:d7:31:57:17:40:a4:6a:8a:57:96:af:63:
        de:05:14:d4:6d:dc:7b:2b:24:26:17:10:fb:c8:91:d6:a1:1a:
        dc:be:e1:ae:d8:99:4d:4d:41:8f:37:5c:41:ae:ed:4e:a2:57:
        17:39:0a:18:05:7b:cc:e7:00:61:b4:cf:55:a3:e8:aa:77:be:
        d1:31:3c:c6:0f:15:ef:3e:f4:8e:b8:a0:f6:7a:53:01:47:d4:
        7a:96:87:7e:6c:c9:97:e2:8a:3e:99:9e:0a:7a:26:06:f7:92:
        33:fe:5b:75:21:e6:17:52:ba:9a:fc:0e:93:db:21:b8:be:13:
        ac:8a:b9:b1:b9:f2:5a:f2:88:3a:bb:fd:a0:0d:c3:4e:87:92:
        5e:4d:87:eb:be:63:7e:3b:38:69:17:08:39:7b:7b:23:27:dc:
        4c:2c:db:af:9b:b1:84:f2:26:c4:1b:aa:db:6c:4f:91:5a:a2:
        84:75:90:9e:75:56:ac:d7:1a:ec:d1:99:09:47:9f:db:03:b6:
        b7:20:34:00:f4:57:9a:86
```