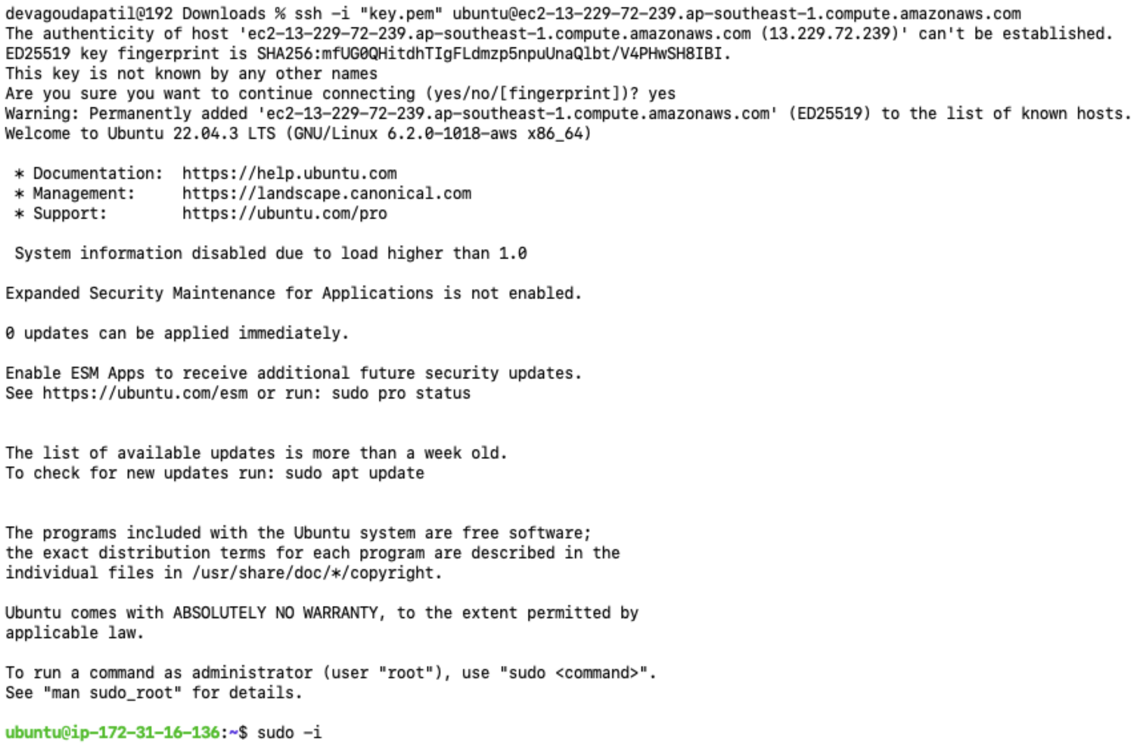
Friday, 1 March 2024

Generate OpenSSL Certificate on EC2 Instance

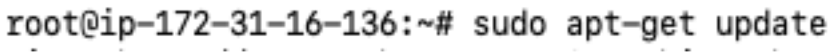
Launch an EC2 instance and connect to it.



```
devagoudapatil@192 Downloads % ssh -i "key.pem" ubuntu@ec2-13-229-72-239.ap-southeast-1.compute.amazonaws.com
The authenticity of host 'ec2-13-229-72-239.ap-southeast-1.compute.amazonaws.com (13.229.72.239)' can't be established.
ED25519 key fingerprint is SHA256:mfUG0QHitdhTIgFLdmzp5npuUnaQlbt/V4PHwSH8IBI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-229-72-239.ap-southeast-1.compute.amazonaws.com' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-1018-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information disabled due to load higher than 1.0

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-16-136:~$ sudo -i
```

First update all packages.

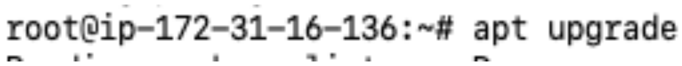
#sudo apt-get update



```
root@ip-172-31-16-136:~# sudo apt-get update
```

Upgrade

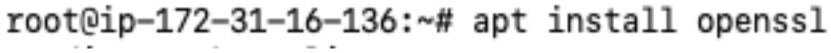
#apt upgrade



```
root@ip-172-31-16-136:~# apt upgrade
```

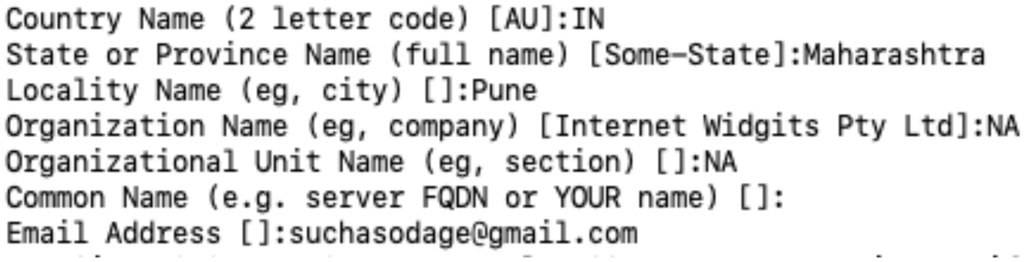
Install open ssl on EC2 instance using following command.

#apt install openssl



```
root@ip-172-31-16-136:~# apt install openssl
```

After installing openssl you need to fill some detail as shown in following image.

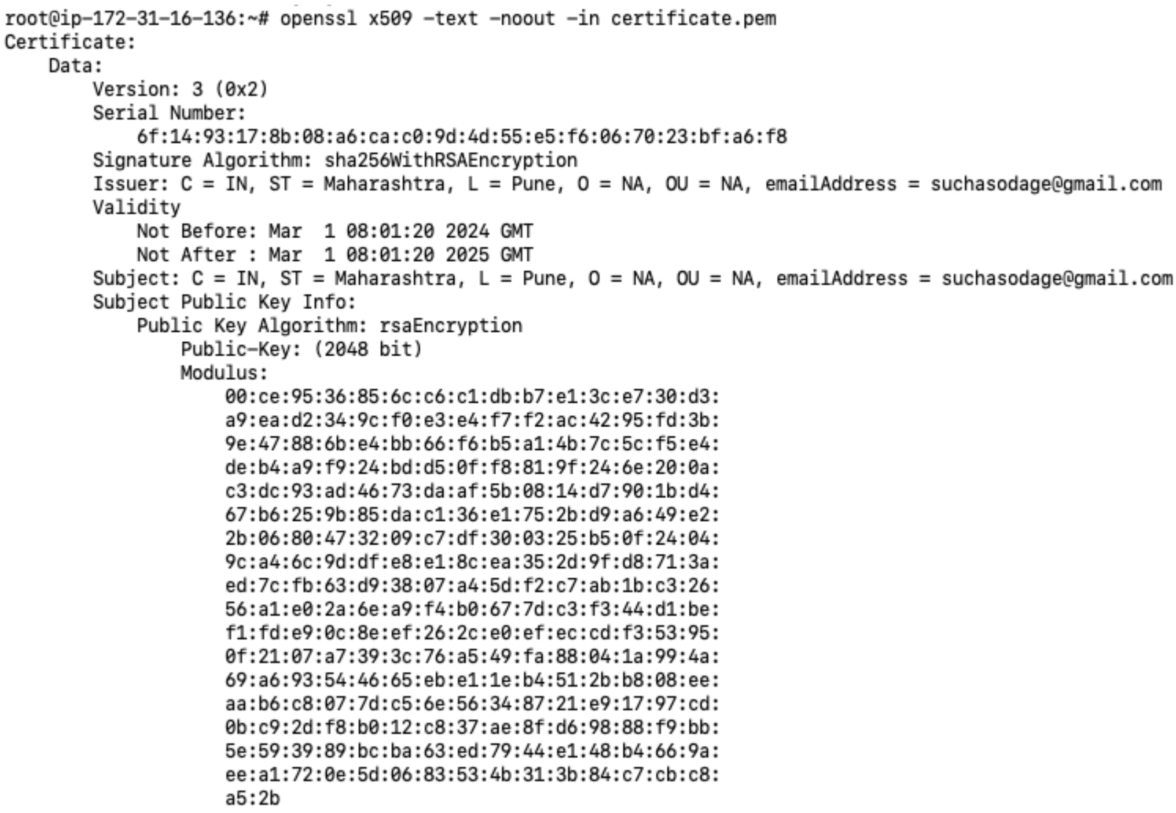


```
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:Maharashtra
Locality Name (eg, city) []:Pune
Organization Name (eg, company) [Internet Widgits Pty Ltd]:NA
Organizational Unit Name (eg, section) []:NA
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:suchasodage@gmail.com
```

You can generate a temporary self signed cert if you want to test locally. By running following command you can generate certificate.

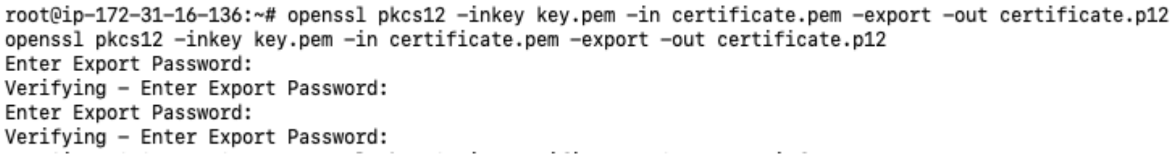
#openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365 -out certificate.pem

#openssl x509 -text -noout -in certificate.pem



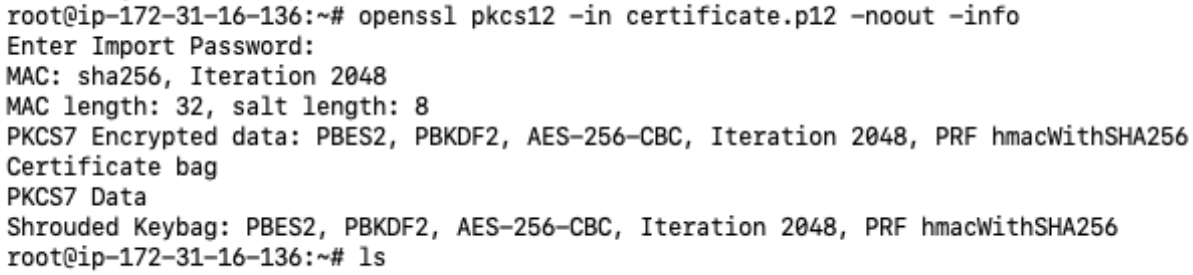
```
root@ip-172-31-16-136:~# openssl x509 -text -noout -in certificate.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            6f:14:93:17:8b:08:a6:ca:c0:9d:4d:55:e5:f6:06:70:23:bf:a6:f8
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = IN, ST = Maharashtra, L = Pune, O = NA, OU = NA, emailAddress = suchasodage@gmail.com
        Validity
            Not Before: Mar  1 08:01:20 2024 GMT
            Not After : Mar  1 08:01:20 2025 GMT
        Subject: C = IN, ST = Maharashtra, L = Pune, O = NA, OU = NA, emailAddress = suchasodage@gmail.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ce:95:36:85:6c:c6:c1:db:b7:e1:3c:e7:30:d3:
                    a9:ea:d2:34:9c:f0:e3:e4:f7:f2:ac:42:95:fd:3b:
                    9e:47:88:6b:e4:bb:66:f6:b5:a1:4b:7c:5c:f5:e4:
                    de:b4:a9:f9:24:bd:d5:0f:f8:81:9f:24:6e:20:0a:
                    c3:dc:93:ad:46:73:da:af:5b:08:14:d7:90:1b:d4:
                    67:b6:25:9b:85:da:c1:36:e1:75:2b:d9:a6:49:e2:
                    2b:06:80:47:32:09:c7:df:30:03:25:b5:0f:24:04:
                    9c:a4:6c:9d:df:e8:e1:8c:ea:35:2d:9f:d8:71:3a:
                    ed:7c:fb:63:d9:38:07:a4:5d:f2:c7:ab:1b:c3:26:
                    56:a1:e0:2a:6e:a9:f4:b0:67:7d:c3:f3:44:d1:be:
                    f1:fd:e9:0c:8e:ef:26:2c:e0:ef:ec:cd:f3:53:95:
                    0f:21:07:a7:39:3c:76:a5:49:fa:88:04:1a:99:4a:
                    69:a6:93:54:46:65:eb:e1:1e:b4:51:2b:b8:08:ee:
                    aa:b6:c8:07:7d:c5:6e:56:34:87:21:e9:17:97:cd:
                    0b:c9:2d:f8:b0:12:c8:37:ae:8f:d6:98:88:f9:bb:
                    5e:59:39:89:bc:ba:63:ed:79:44:e1:48:b4:66:9a:
                    ee:a1:72:0e:5d:06:83:53:4b:31:3b:84:c7:cb:c8:
                    a5:2b
```

#openssl pkcs12 -inkey key.pem -in certificate.pem -export -out certificate.p12



```
root@ip-172-31-16-136:~# openssl pkcs12 -inkey key.pem -in certificate.pem -export -out certificate.p12
openssl pkcs12 -inkey key.pem -in certificate.pem -export -out certificate.p12
Enter Export Password:
Verifying - Enter Export Password:
Enter Export Password:
Verifying - Enter Export Password:
```

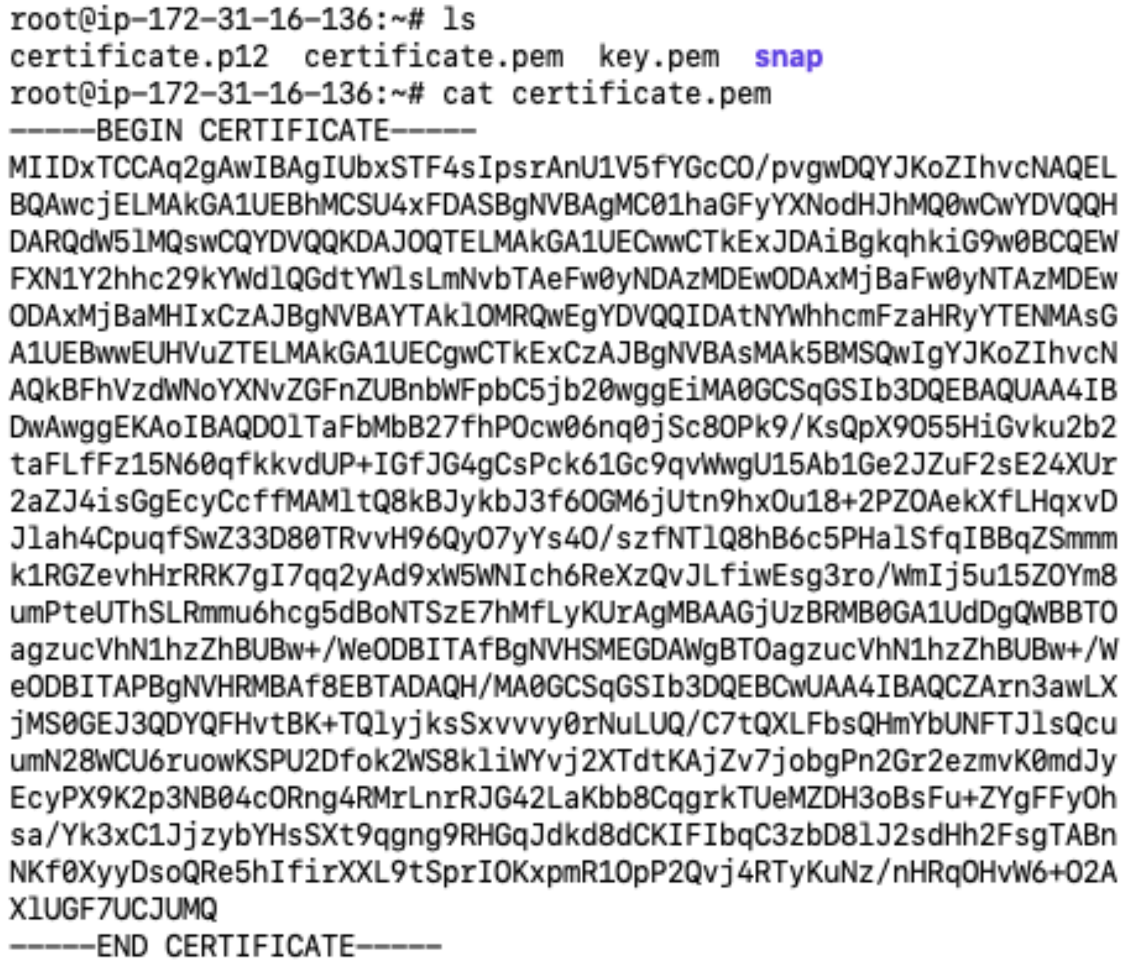
#openssl pkcs12 -in certificate.p12 -noout -info



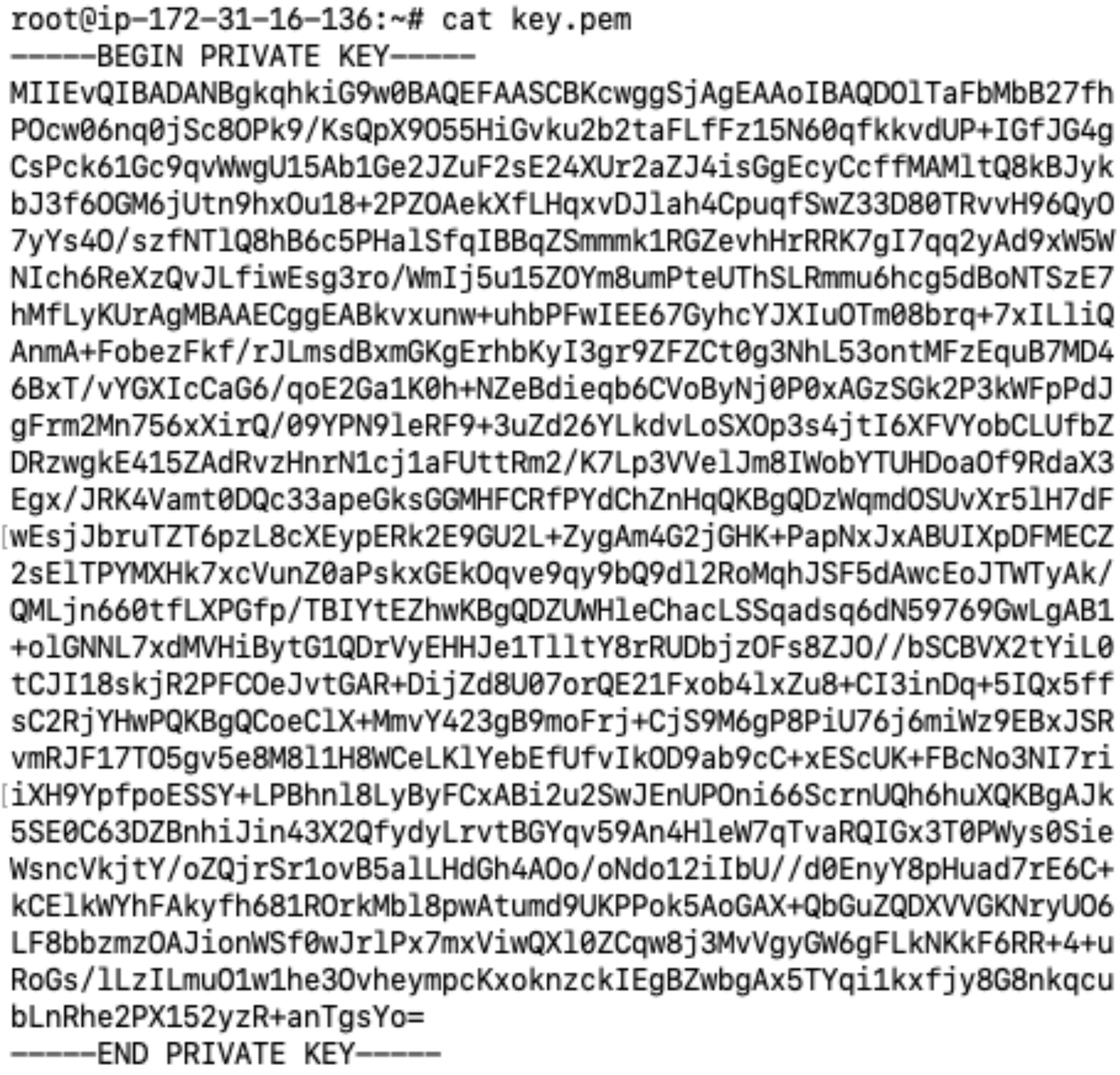
```
root@ip-172-31-16-136:~# openssl pkcs12 -in certificate.p12 -noout -info
Enter Import Password:
MAC: sha256, Iteration 2048
MAC length: 32, salt length: 8
PKCS7 Encrypted data: PBES2, PBKDF2, AES-256-CBC, Iteration 2048, PRF hmacWithSHA256
Certificate bag
PKCS7 Data
Shrouded Keybag: PBES2, PBKDF2, AES-256-CBC, Iteration 2048, PRF hmacWithSHA256
root@ip-172-31-16-136:~# ls
```

Sign-in into your AWS account and navigate to AWS Certificate Manager Service console. Click on “Import Certificate”.

Go to your instance and copy certificate body and key.



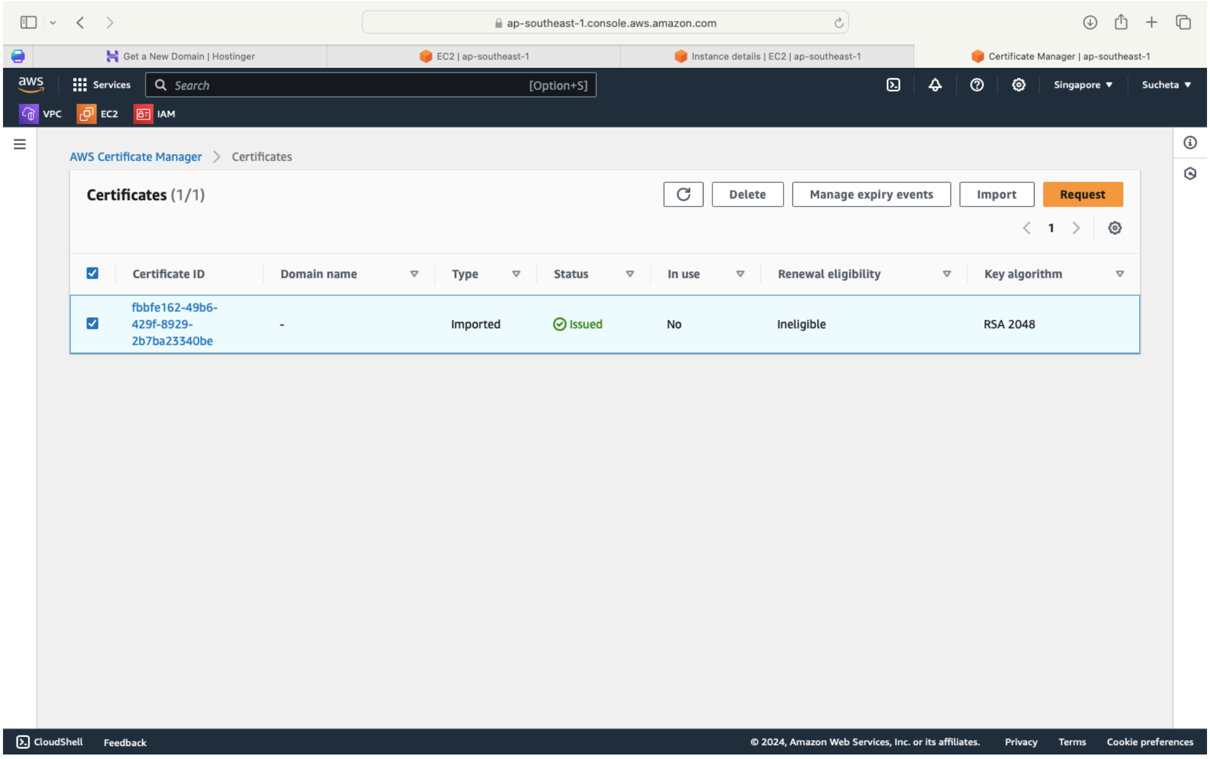
```
root@ip-172-31-16-136:~# ls
certificate.p12  certificate.pem  key.pem  snap
root@ip-172-31-16-136:~# cat certificate.pem
-----BEGIN CERTIFICATE-----
MIIDxTCCAq2gAwIBAgIUbxSTF4sIpsrAnU1V5fYGcCO/pvgwDQYJKoZIhvcNAQEL
BQAwcjELMAkGA1UEBhMCSU4xFDASBgNVBAgMC01haGFyYXNodHJhMQ0wCwYDVQQH
DARQdW5lMQswCQYDVQQKDAJOQTELMAkGA1UECwwCTkExJDAiBgkqhkiG9w0BCQEW
FXN1Y2hhc29kYWdlQGdtYWlsLmNvbTAeFw0yNDAzMDEwODAxMjBaFw0yNTAzMDEw
ODAxMjBaMHIxCzAJBgNVBAYTAklOMRQwEgYDVQQIDAtNYWhhcmFzaHRyYTENMAsG
A1UEBwwEUHVuZTELMAkGA1UECgwCTkExCzAJBgNVBAsMAk5BMSQwIgYJKoZIhvcN
AQkBFhVzdWNoYXNvZGFnZUBnbWFpbC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQDOlTaFbMbB27fhPOcw06nq0jSc8OPk9/KsQpX9O55HiGvku2b2
taFLfFz15N60qfkkvdUP+IGfJG4gCsPck61Gc9qvWwgU15Ab1Ge2JZuF2sE24XUr
2aZJ4isGgEcyCcffMAMltQ8kBJykbJ3f6OGM6jUtn9hxOu18+2PZOAekXfLHqxvD
Jlah4CpuqfSwZ33D80TRvvH96QyO7yYs4O/szfNTlQ8hB6c5PHalSfqIBBqZSmmm
k1RGZevhHrRRK7gI7qq2yAd9xW5WNIch6ReXzQvJLfiwEsg3ro/WmIj5u15ZOYm8
umPteUThSLRmmu6hcg5dBoNTSzE7hMfLyKUrAgMBAAGjUzBRMB0GA1UdDgQWBBTO
agzucVhN1hzZhBUBw+/WeODBITAfBgNVHSMEGDAWgBTOagzucVhN1hzZhBUBw+/W
eODBITAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQCZArn3awLX
jMS0GEJ3QDYQFHvtBK+TQlyjksSxvvvy0rNuLUQ/C7tQXLFbsQHmYbUNFTJlsQcu
umN28WCU6ruowKSPU2Dfok2WS8kliWYvj2XTdtKAjZv7jobgPn2Gr2ezmvK0mdJy
EcyPX9K2p3NB04cORng4RMrLnrRJG42LaKbb8CqgrkTUeMZDH3oBsFu+ZYgFFyOh
sa/Yk3xC1JjzybYHsSXt9qgng9RHGqJdkd8dCKIFIbqC3zbD8lJ2sdHh2FsgTABn
NKf0XyyDsoQRe5hIfirXXL9tSprIOKxpmR1OpP2Qvj4RTyKuNz/nHRqOHvW6+O2A
XlUGF7UCJUMQ
-----END CERTIFICATE-----
```



```
root@ip-172-31-16-136:~# cat key.pem
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDOlTaFbMbB27fh
POcw06nq0jSc8OPk9/KsQpX9O55HiGvku2b2taFLfFz15N60qfkkvdUP+IGfJG4g
CsPck61Gc9qvWwgU15Ab1Ge2JZuF2sE24XUr2aZJ4isGgEcyCcffMAMltQ8kBJyk
bJ3f6OGM6jUtn9hxOu18+2PZOAekXfLHqxvDJlah4CpuqfSwZ33D80TRvvH96QyO
7yYs4O/szfNTlQ8hB6c5PHalSfqIBBqZSmmmk1RGZevhHrRRK7gI7qq2yAd9xW5W
NIch6ReXzQvJLfiwEsg3ro/WmIj5u15ZOYm8umPteUThSLRmmu6hcg5dBoNTSzE7
hMfLyKUrAgMBAAECggEABkvxunw+uhbPFwIEE67GyhcYJXIuOTm08brq+7xILliQ
AnmA+FobezFkf/rJLmsdBxmGKgErhbKyI3gr9ZFZCt0g3NhL53ontMFzEquB7MD4
6BxT/vYGXIcCaG6/qoE2Ga1K0h+NZeBdieqb6CVoByNj0P0xAGzSGk2P3kWFpPdJ
gFrm2Mn756xXirQ/09YPN9leRF9+3uZd26YLkdvLoSXOp3s4jtI6XFVYobCLUfbZ
DRzwgkE415ZAdRvzHnrN1cj1aFUttRm2/K7Lp3VVelJm8IWobYTUHDoaOf9RdaX3
Egx/JRK4Vamt0DQc33apeGksGGMHFCRfPYdChZnHqQKBgQDzWqmdOSUvXr5lH7dF
wEsjJbruTZT6pzL8cXEypERk2E9GU2L+ZygAm4G2jGHK+PapNxJxABUIXpDFMECZ
2sElTPYMXHk7xcVunZ0aPskxGEkOqve9qy9bQ9dl2RoMqhJSF5dAwcEoJTWTyAk/
QMLjn660tfLXPGfp/TBIYtEZhwKBgQDZUWHleChacLSSqadsq6dN59769GwLgAB1
+olGNNL7xdMVHiBytG1QDrVyEHHJe1TlltY8rRUDbjzOFs8ZJO//bSCBVX2tYiL0
tCJI18skjR2PFCOeJvtGAR+DijZd8U07orQE21Fxob4lxZu8+CI3inDq+5IQx5ff
sC2RjYHwPQKBgQCoeClX+MmvY423gB9moFrj+CjS9M6gP8PiU76j6miWz9EBxJSR
vmRJF17TO5gv5e8M8l1H8WCeLKlYebEfUfvIkOD9ab9cC+xEScUK+FBcNo3NI7ri
iXH9YpfpoESSY+LPBhnl8LyByFCxABi2u2SwJEnUPOni66ScrnUQh6huXQKBgAJk
5SE0C63DZBnhiJin43X2QfydyLrvtBGYqv59An4HleW7qTvaRQIGx3T0PWys0Sie
WsncVkjtY/oZQjrSr1ovB5alLHdGh4AOo/oNdo12iIbU//d0EnyY8pHuad7rE6C+
kCElkWYhFAkyfh681ROrkMbl8pwAtumd9UKPPok5AoGAX+QbGuZQDXVVGKNryUO6
LF8bbzmzOAJionWSf0wJrlPx7mxViwQXl0ZCqw8j3MvVgyGW6gFLkNKkF6RR+4+u
RoGs/lLzILmuO1w1he3OvheympcKxoknzckIEgBZwbgAx5TYqi1kxfjy8G8nkqcu
bLnRhe2PX152yzR+anTgsYo=
-----END PRIVATE KEY-----
```

Paste this key in certificate body and key body fields in AWS Certificate manager.

Click on Next, then review your certificate details and click on Import.


ap-southeast-1.console.aws.amazon.com
Get a New Domain | Hostinger
EC2 | ap-southeast-1
Instance details | EC2 | ap-southeast-1
Certificate Manager | ap-southeast-1
aws
Services
Search
[Option+S]
Singapore ▼
Sucheta ▼
VPC
EC2
IAM
AWS Certificate Manager > Certificates
Delete
Manage expiry events
Import
Request
1
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Certificates (1/1)

☑	Certificate ID	Domain name	Type	Status	In use	Renewal eligibility	Key algorithm
☑	fbbfe162-49b6-429f-8929-2b7ba23340be	-	Imported	✓ Issued	No	Ineligible	RSA 2048