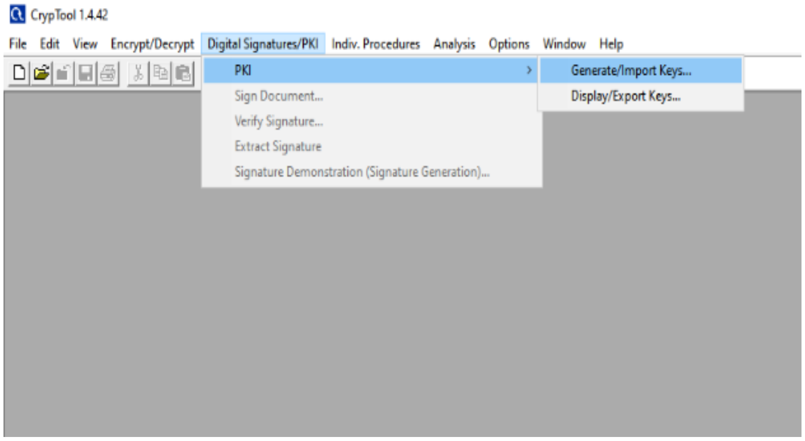
Module:- Public Key Infrastructure Date:- 16/09/2022

Assignment :- 02

CRYPTOOL :-

Practical:- Digital Signature Certificate (DSC)

Step- 1:- Open the Cryptool and it's show many option. Then we can select Digital Signature/PKI → PKI → Generate/Import Keys.



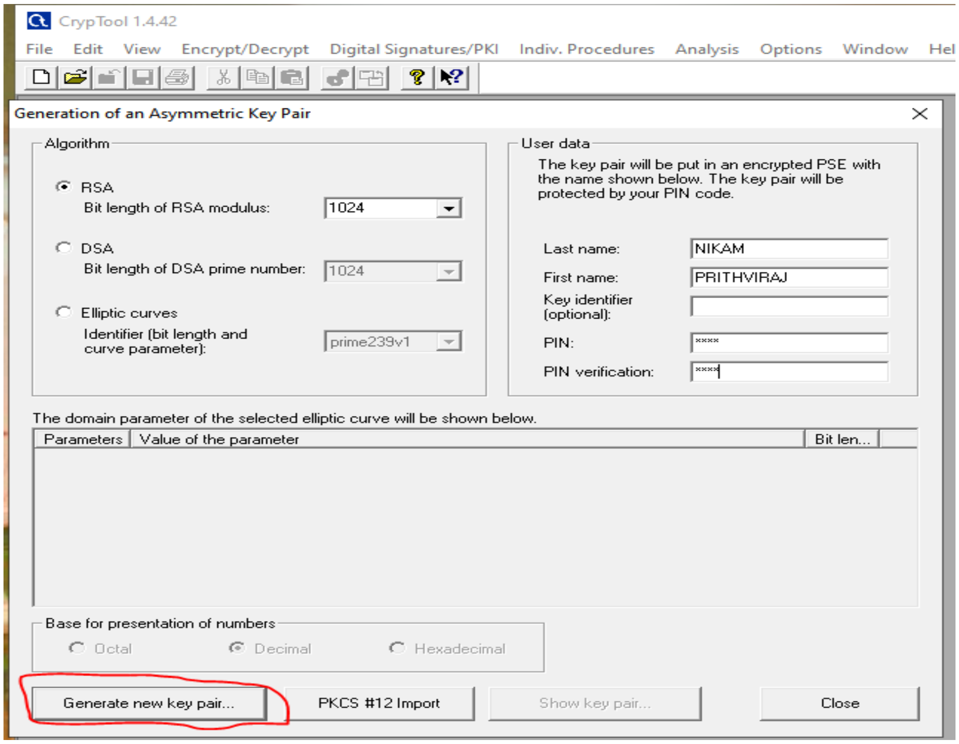
Step-2:- this step show Generation of an Asymmetric Key Pair. In this Key pair show's three radio button then we can select RSA ,his parallel way user data show's text box Last Name, First Name, key Identifier(optional) and PIN .we can put all data in text box and Generate New key pair.

Last Name :- NIKAM

First Name:- PRITHVIRAJ

Key Identifier(optional):-

PIN:- ****


CrypTool 1.4.42
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Hel
Generate new key pair...
PKCS #12 Import
Show key pair...
Close

Generation of an Asymmetric Key Pair

Algorithm

● RSA
Bit length of RSA modulus: 1024

○ DSA
Bit length of DSA prime number: 1024

○ Elliptic curves
Identifier (bit length and curve parameter): prime239v1

User data

The key pair will be put in an encrypted PSE with the name shown below. The key pair will be protected by your PIN code.

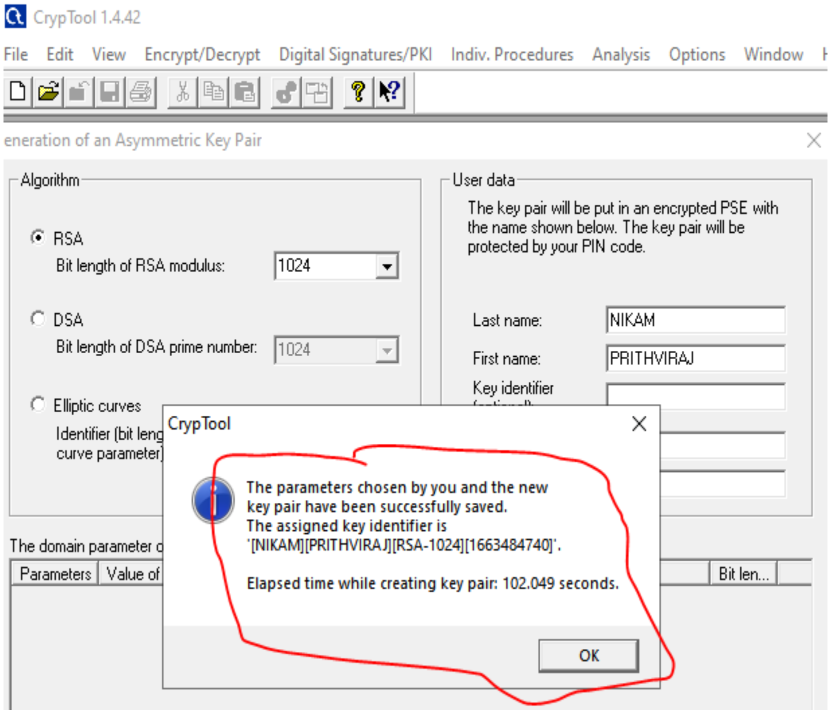
Last name: NIKAM
First name: PRITHVIRAJ
Key identifier (optional):
PIN: ****
PIN verification: ****

The domain parameter of the selected elliptic curve will be shown below.

Parameters	Value of the parameter	Bit len...

Base for presentation of numbers
○ Octal ● Decimal ○ Hexadecimal

Step-3:- Key Generater opening new popup that show your Key pair successfully created.


CrypTool 1.4.42
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window H
eneration of an Asymmetric Key Pair
CrypTool
OK

Algorithm

● RSA
Bit length of RSA modulus: 1024

○ DSA
Bit length of DSA prime number: 1024

○ Elliptic curves
Identifier (bit leng
curve parameter)

User data

The key pair will be put in an encrypted PSE with the name shown below. The key pair will be protected by your PIN code.

Last name: NIKAM
First name: PRITHVIRAJ
Key identifier

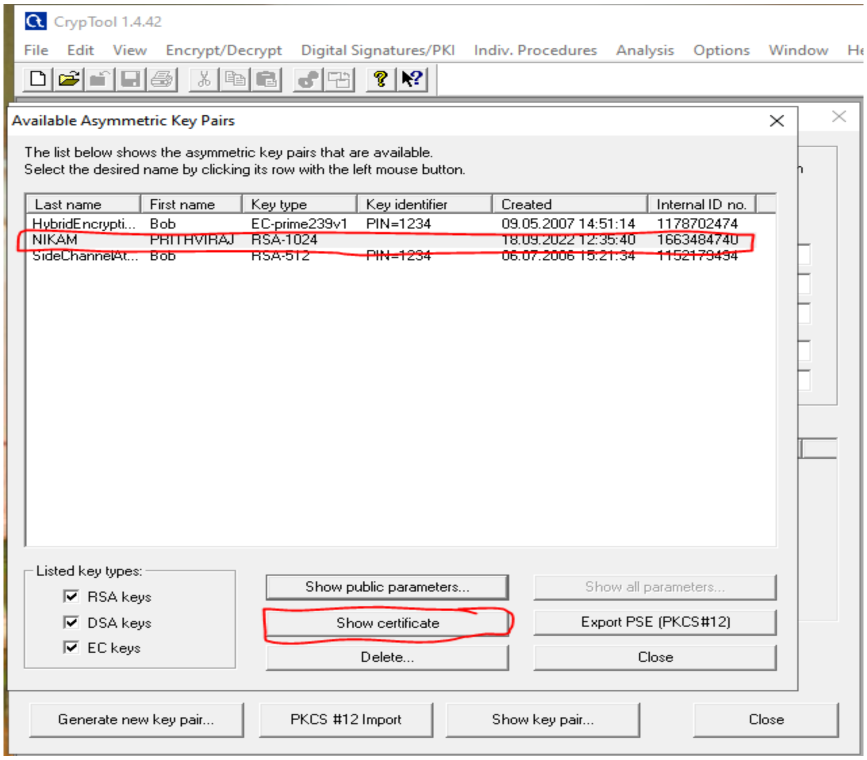
The domain parameter o

Parameters	Value of	Bit len...

The parameters chosen by you and the new key pair have been successfully saved.
The assigned key identifier is '[NIKAM][PRITHVIRAJ][RSA-1024][1663484740]'.

Elapsed time while creating key pair: 102.049 seconds.

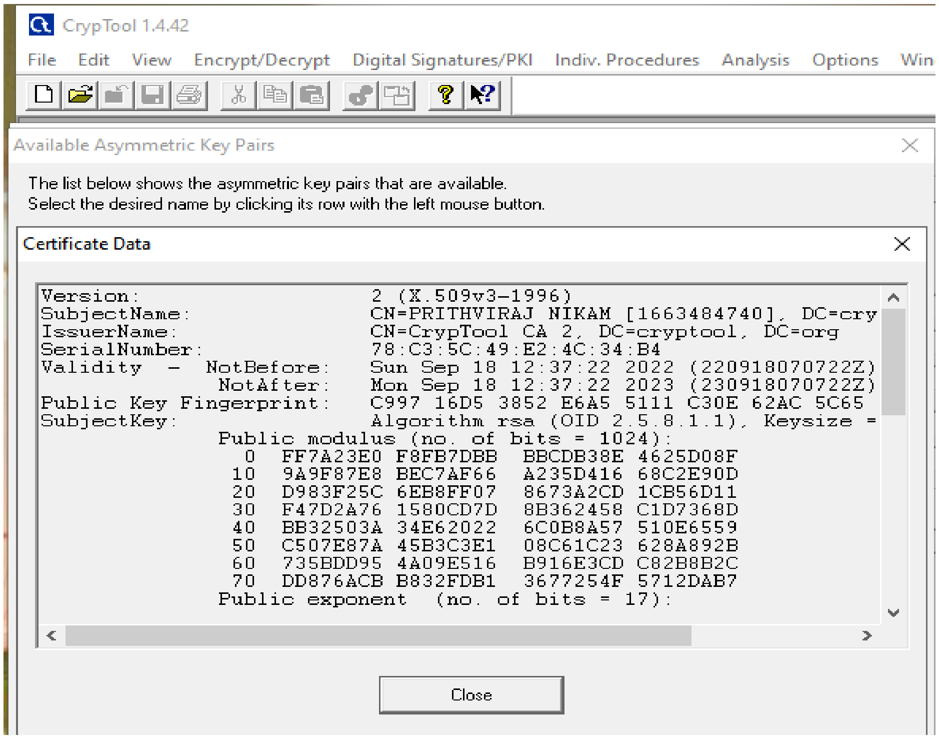
Step-4 :- After key Creation, new window show’s available Asymmetric key pair and we can select show certificate option.



The list below shows the asymmetric key pairs that are available.
Select the desired name by clicking its row with the left mouse button.

Last name	First name	Key type	Key identifier	Created	Internal ID no.
HybridEncrypti...	Bob	EC-prime239v1	PIN=1234	09.05.2007 14:51:14	1178702474
NIKAM	PRITHVIRAJ	RSA-1024		18.09.2022 12:35:40	1663484740
SideChannelAt...	Bob	RSA-512	PIN=1234	06.07.2006 15:21:34	1152179494

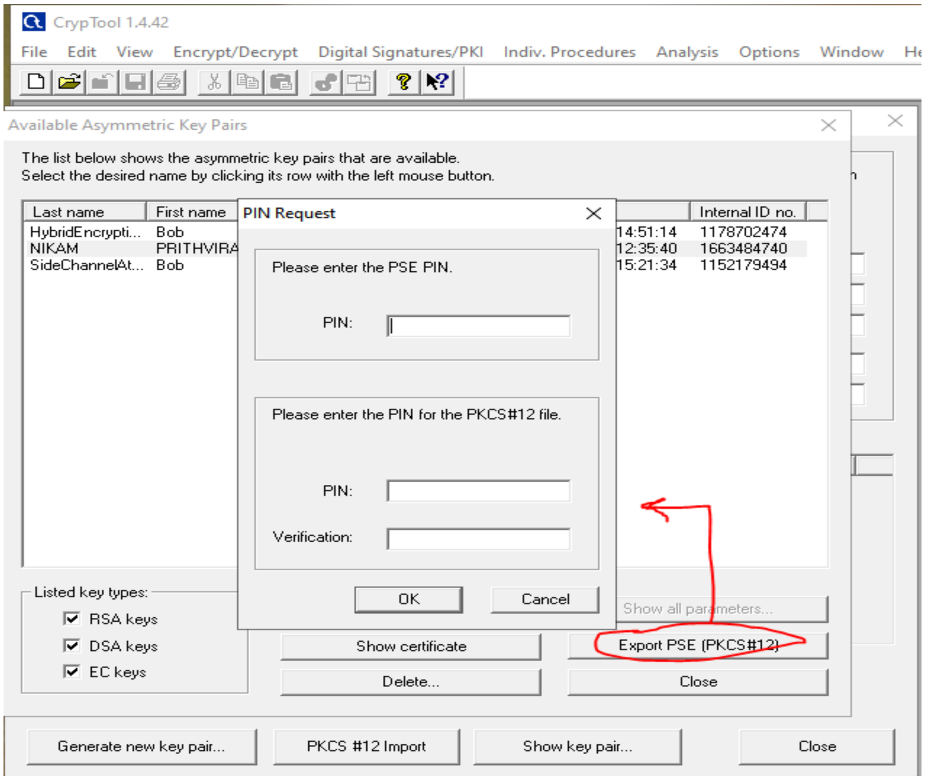
Step- 5 :- The Certificate show all Certificate data .


CrypTool 1.4.42
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Win
Available Asymmetric Key Pairs
Certificate Data
Close

The list below shows the asymmetric key pairs that are available.
Select the desired name by clicking its row with the left mouse button.

```
Version:                    2 (X.509v3-1996)
SubjectName:                CN=PRITHVIRAJ NIKAM [1663484740], DC=cry
IssuerName:                 CN=CrypTool CA 2, DC=cryptool, DC=org
SerialNumber:               78:C3:5C:49:E2:4C:34:B4
Validity  -  NotBefore:     Sun Sep 18 12:37:22 2022 (220918070722Z)
             NotAfter:      Mon Sep 18 12:37:22 2023 (230918070722Z)
Public Key Fingerprint:     C997 16D5 3852 E6A5 5111 C30E 62AC 5C65
SubjectKey:                 Algorithm rsa (OID 2.5.8.1.1), Keysize =
              Public modulus (no. of bits = 1024):
                 0  FF7A23E0 F8FB7DBB  BBCDB38E 4625D08F
                10  9A9F87E8 BEC7AF66  A235D416 68C2E90D
                20  D983F25C 6EB8FF07  8673A2CD 1CB56D11
                30  F47D2A76 1580CD7D  8B362458 C1D7368D
                40  BB32503A 34E62022  6C0B8A57 510E6559
                50  C507E87A 45B3C3E1  08C61C23 628A892B
                60  735BDD95 4A09E516  B916E3CD C82B8B2C
                70  DD876ACB B832FDB1  3677254F 5712DAB7
              Public exponent  (no. of bits = 17):
```

Step-6:- Back to step-4 and select Export PSE(PKCS#12) and tool open new popup that show three text box PSE PIN and PKCS File PIN(***) and it's verification. Select ok.



The list below shows the asymmetric key pairs that are available.
Select the desired name by clicking its row with the left mouse button.

Last name	First name		Internal ID no.
HybridEncrypti...	Bob	14:51:14	1178702474
NIKAM	PRITHVIRA	12:35:40	1663484740
SideChannelAt...	Bob	15:21:34	1152179494

Please enter the PSE PIN.

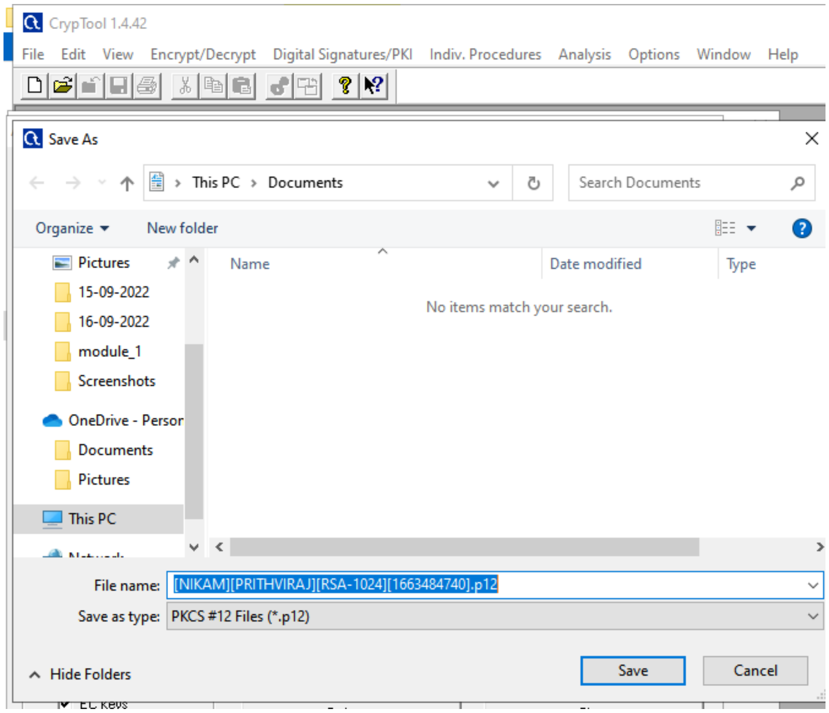
PIN:

Please enter the PIN for the PKCS#12 file.

PIN:

Verification:

Step- 7:- After clicking ok option opening System Directory. We can Select any folder to store Certificate.

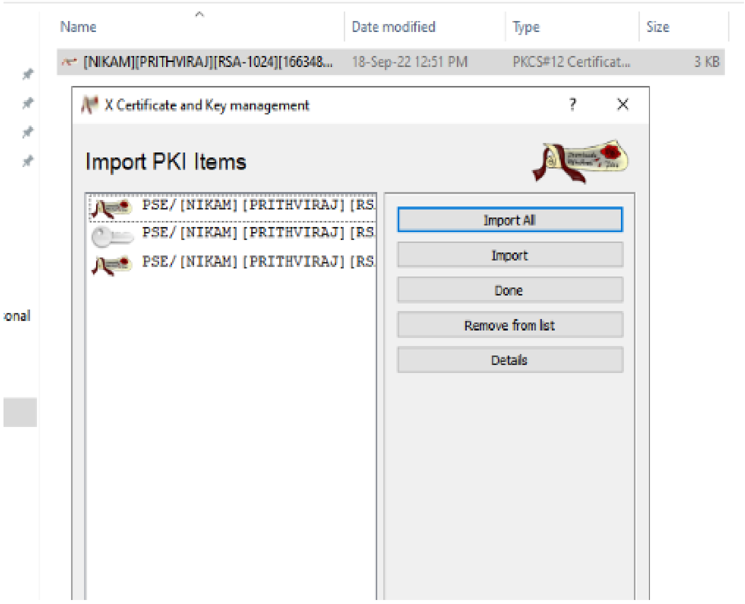


No items match your search.

File name: [NIKAM][PRITHVIRAJ][RSA-1024][1663484740].p12

Save as type: PKCS #12 Files (*.p12)

Step- 8:- After saving the certificate**.** Select the certificate put PSE Password and open new window show's three PKI items.



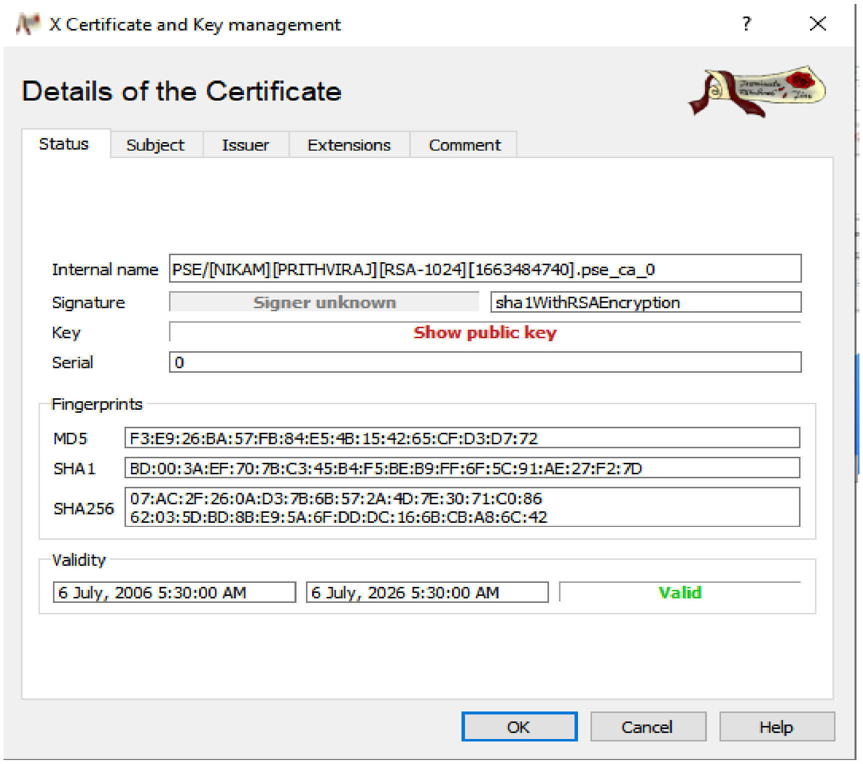
Name	Date modified	Type	Size
[NIKAM][PRITHVIRAJ][RSA-1024][166348...	18-Sep-22 12:51 PM	PKCS#12 Certificat...	3 KB

X Certificate and Key management

Import PKI Items

- PSE/ [NIKAM] [PRITHVIRAJ] [RS
- PSE/ [NIKAM] [PRITHVIRAJ] [RS
- PSE/ [NIKAM] [PRITHVIRAJ] [RS

Step-9 :- PKI Item show Key details and Certificate Details.



X Certificate and Key management

Details of the Certificate

Internal name: PSE/[NIKAM][PRITHVIRAJ][RSA-1024][1663484740].pse_ca_0

Signature: Signer unknown | sha1WithRSAEncryption

Key: Show public key

Serial: 0

Fingerprints

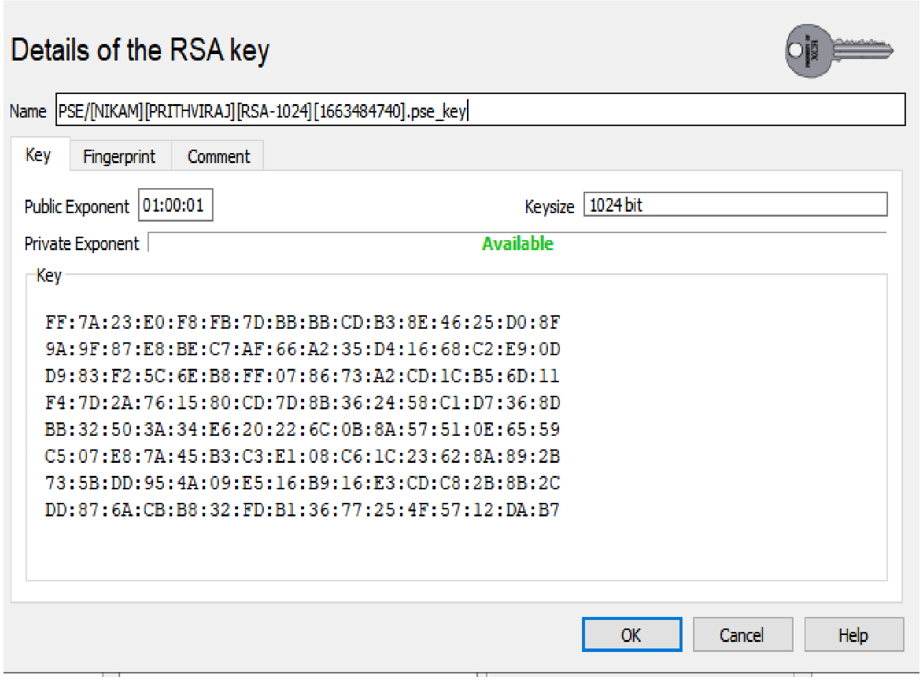
MD5: F3:E9:26:BA:57:FB:84:E5:4B:15:42:65:CF:D3:D7:72

SHA1: BD:00:3A:EF:70:7B:C3:45:B4:F5:BE:B9:FF:6F:5C:91:AE:27:F2:7D

SHA256: 07:AC:2F:26:0A:D3:7B:6B:57:2A:4D:7E:30:71:C0:86
62:03:5D:BD:8B:E9:5A:6F:DD:DC:16:6B:CB:A8:6C:42

Validity

6 July, 2006 5:30:00 AM | 6 July, 2026 5:30:00 AM | Valid



Details of the RSA key

Name PSE/[NIKAM][PRITHVIRAJ][RSA-1024][1663484740].pse_key

Public Exponent 01:00:01

Keysize 1024 bit

Private Exponent Available

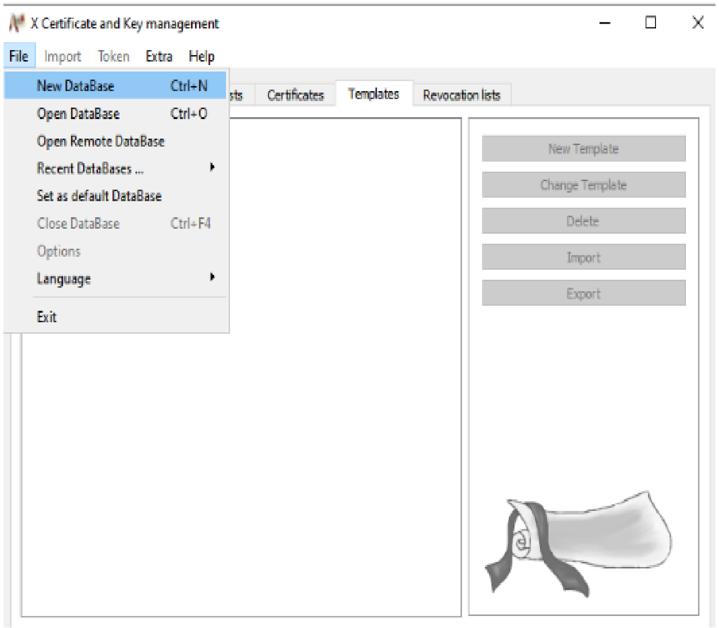
Key

```
FF:7A:23:E0:F8:FB:7D:BB:BB:CD:B3:8E:46:25:D0:8F
9A:9F:87:E8:BE:C7:AF:66:A2:35:D4:16:68:C2:E9:0D
D9:83:F2:5C:6E:B8:FF:07:86:73:A2:CD:1C:B5:6D:11
F4:7D:2A:76:15:80:CD:7D:8B:36:24:58:C1:D7:36:8D
BB:32:50:3A:34:E6:20:22:6C:0B:8A:57:51:0E:65:59
C5:07:E8:7A:45:B3:C3:E1:08:C6:1C:23:62:8A:89:2B
73:5B:DD:95:4A:09:E5:16:B9:16:E3:CD:C8:2B:8B:2C
DD:87:6A:CB:B8:32:FD:B1:36:77:25:4F:57:12:DA:B7
```

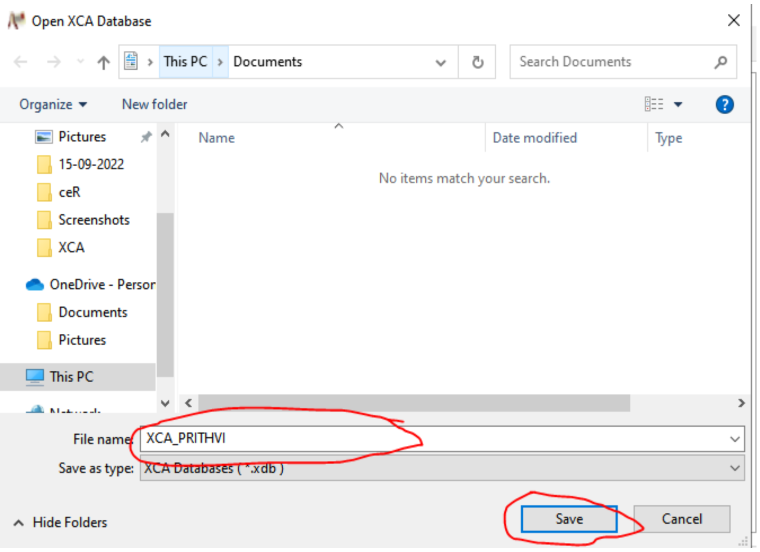
XCA TOOL:-

PRACTICAL:- Digital Signature Certificate (DSC)

Step – 1:- Open XCA tool and select New Database Option.



Save New Data Base file into any folder of system.

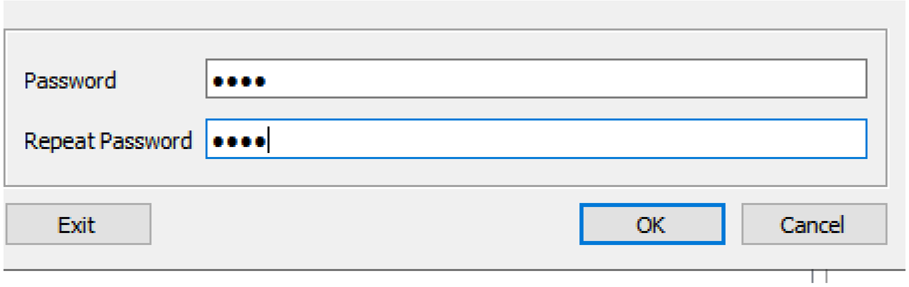


No items match your search.

File name: XCA_PRITHVI

Save as type: XCA Databases (*.xdb)

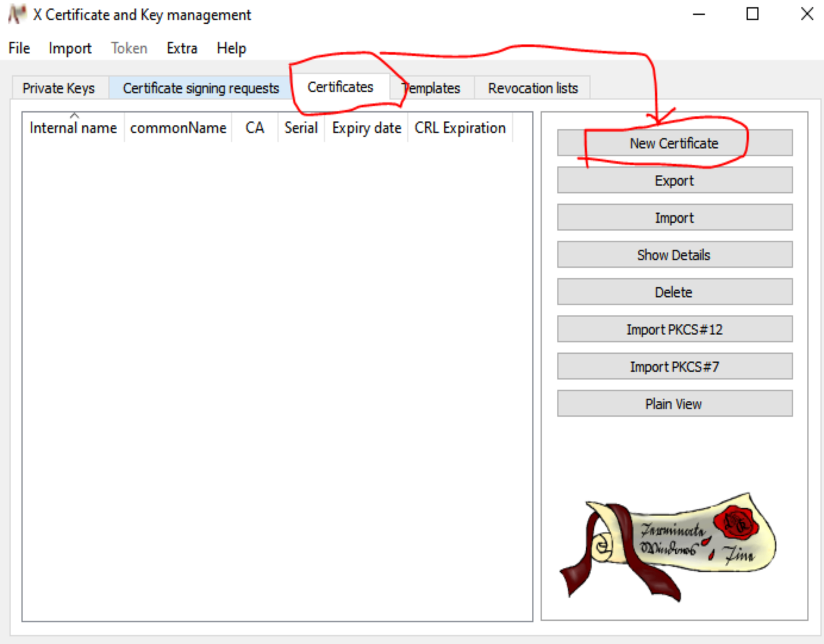
After Saving Set Password.



Password: ••••

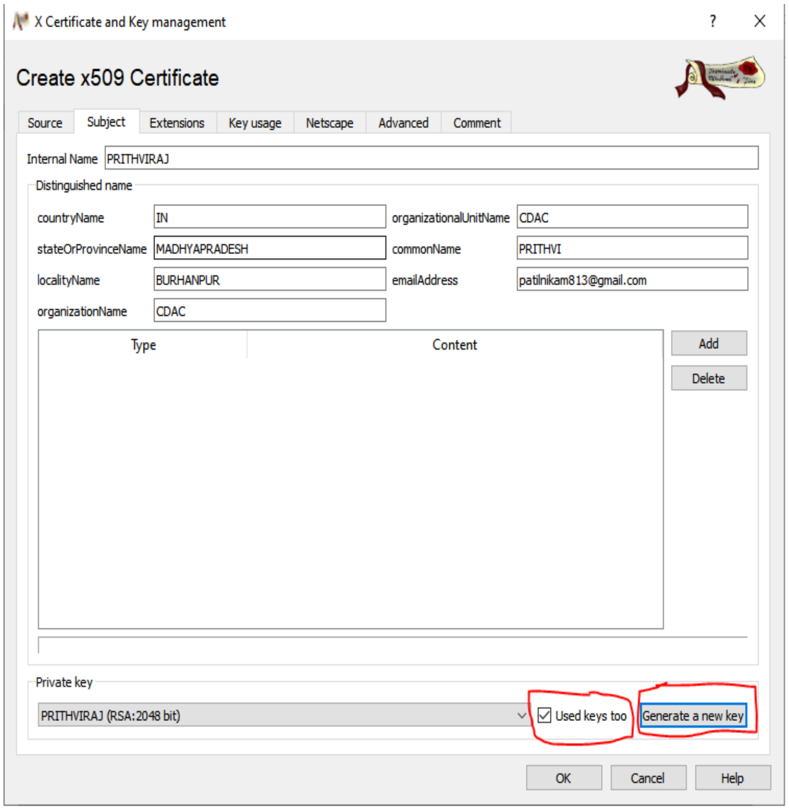
Repeat Password: ••••

Step -2:-Now select Certificate option and then select New certificate option.



Step -3:- Now **,** after opening new certificate in XCA tool open new window and Create Certificate that have many text box such as.
Internal name:- PRITHVIRAJ
Country name:- IN
State :- MADHYAPRADESH
Locality :- BURHANPUR
Organization name :- CDAC
Organization Unit Nmae :- CDAC
Common Name:- PRITHVI
Email-ID :- patilnikam813@gmail.com

And then we can select Generate new Key option.



X Certificate and Key management

Create x509 Certificate

Internal Name PRITHVIRAJ

Distinguished name

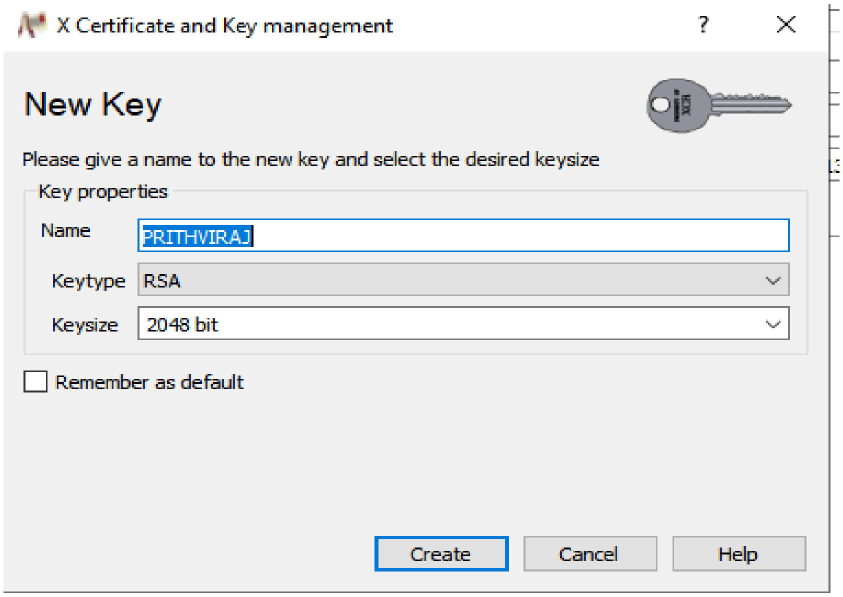
countryName IN
stateOrProvinceName MADHYAPRADESH
localityName BURHANPUR
organizationName CDAC
organizationalUnitName CDAC
commonName PRITHVI
emailAddress patilnikam813@gmail.com

Private key

PRITHVIRAJ (RSA:2048 bit)

☑ Used keys too

New Key generator generate is following image .



X Certificate and Key management

New Key

Please give a name to the new key and select the desired keysize

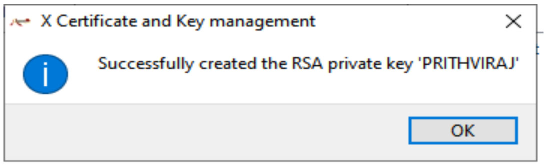
Key properties

Name: PRITHVIRAJ

Keytype: RSA

Keysize: 2048 bit

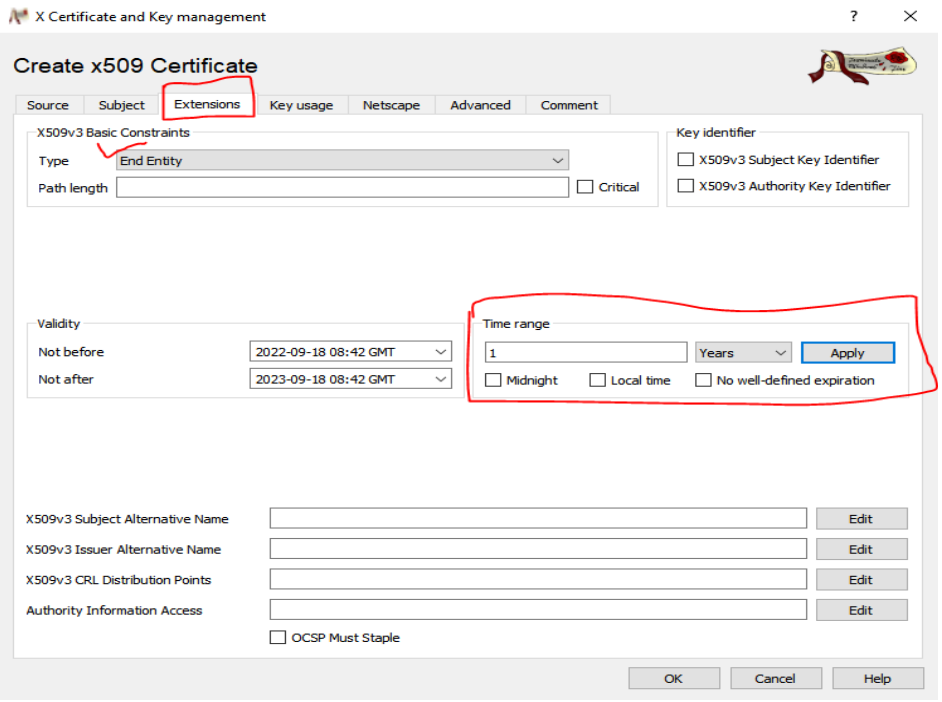
□ Remember as default



X Certificate and Key management

Successfully created the RSA private key 'PRITHVIRAJ'

Step -4 :- After we can select Extensions when we can select End Entity and Time Period



X Certificate and Key management

Create x509 Certificate

X509v3 Basic Constraints

Type: End Entity

Path length: □ Critical

Key identifier

□ X509v3 Subject Key Identifier

□ X509v3 Authority Key Identifier

Validity

Not before: 2022-09-18 08:42 GMT

Not after: 2023-09-18 08:42 GMT

Time range

1 Years Apply

□ Midnight □ Local time □ No well-defined expiration

X509v3 Subject Alternative Name — Edit

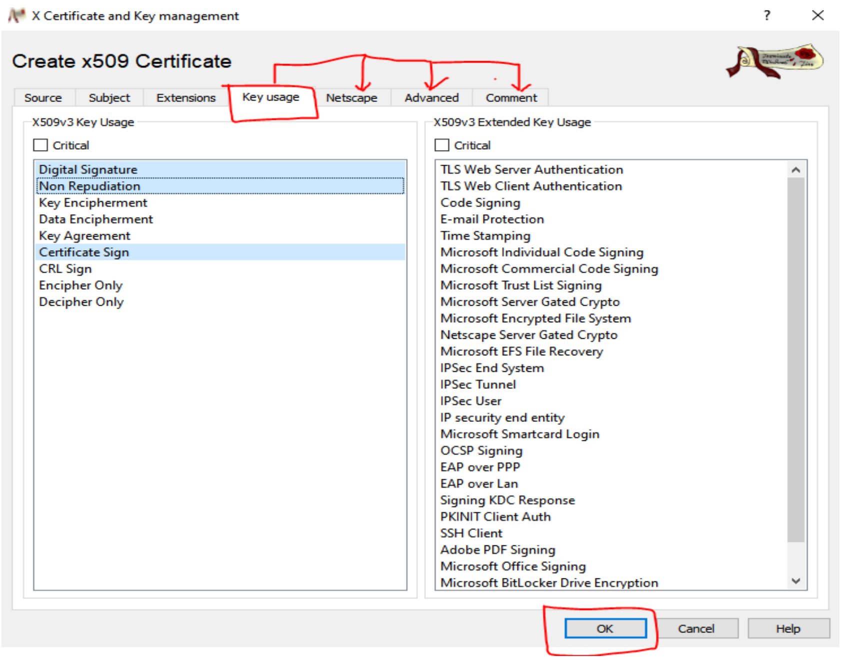
X509v3 Issuer Alternative Name — Edit

X509v3 CRL Distribution Points — Edit

Authority Information Access — Edit

□ OCSP Must Staple

Step- 5:- Now we go to Key usage Option when we select Digital signature ,Non Repudiation and Certificate Sign option and last select ok.



Create x509 Certificate

X509v3 Key Usage

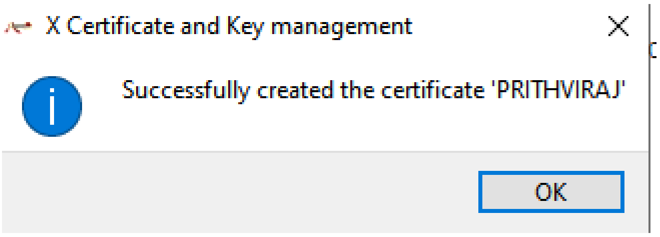
□ Critical

- Digital Signature
- Non Repudiation
- Key Encipherment
- Data Encipherment
- Key Agreement
- Certificate Sign
- CRL Sign
- Encipher Only
- Decipher Only

X509v3 Extended Key Usage

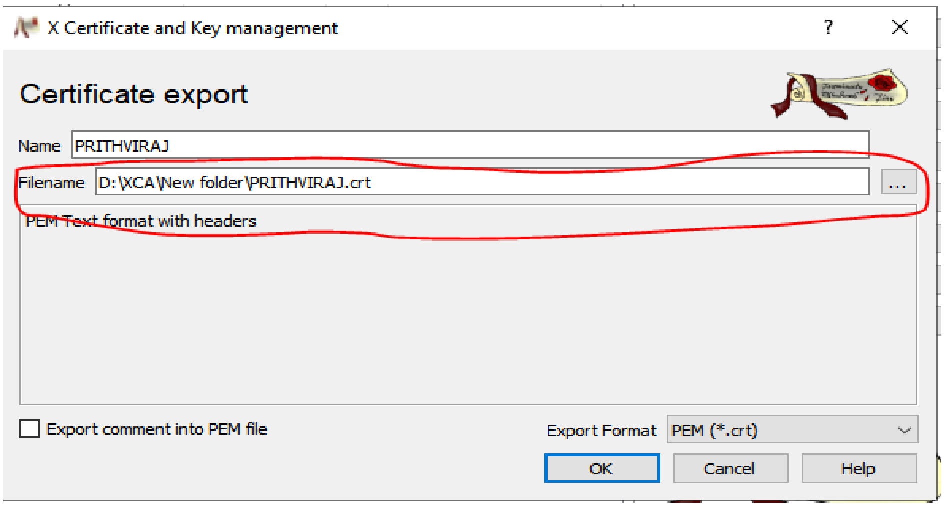
□ Critical

- TLS Web Server Authentication
- TLS Web Client Authentication
- Code Signing
- E-mail Protection
- Time Stamping
- Microsoft Individual Code Signing
- Microsoft Commercial Code Signing
- Microsoft Trust List Signing
- Microsoft Server Gated Crypto
- Microsoft Encrypted File System
- Netscape Server Gated Crypto
- Microsoft EFS File Recovery
- IPSec End System
- IPSec Tunnel
- IPSec User
- IP security end entity
- Microsoft Smartcard Login
- OCSP Signing
- EAP over PPP
- EAP over Lan
- Signing KDC Response
- PKINIT Client Auth
- SSH Client
- Adobe PDF Signing
- Microsoft Office Signing
- Microsoft BitLocker Drive Encryption



Successfully created the certificate 'PRITHVIRAJ'

Step -6 :- After certificate creation open new popup that we can set path.



Certificate export

Name PRITHVIRAJ

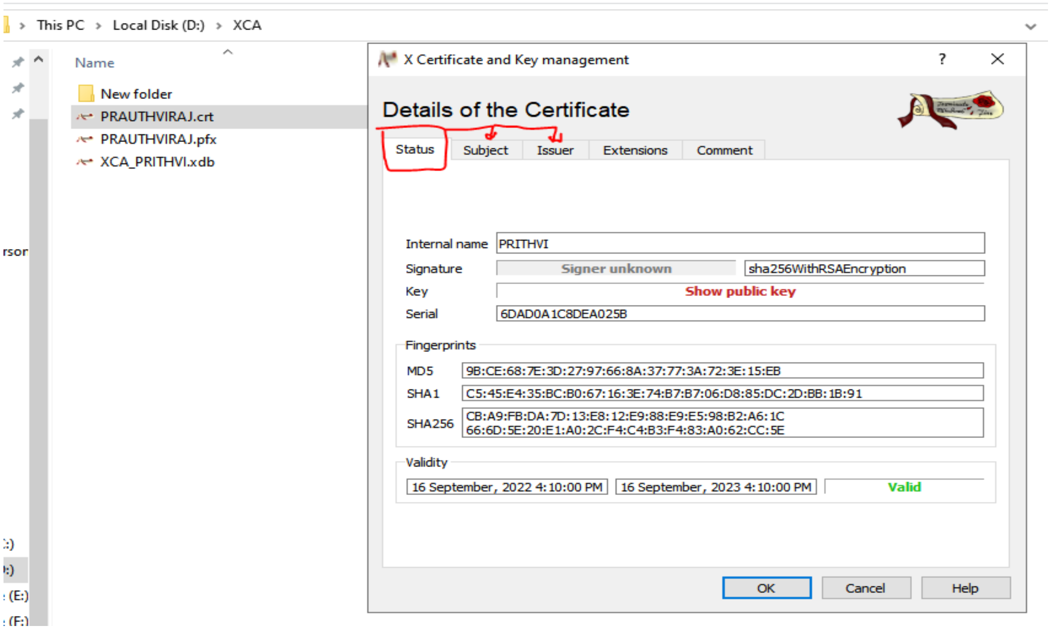
Filename D:\XCA\New folder\PRITHVIRAJ.crt

PEM Text format with headers

□ Export comment into PEM file

Export Format PEM (*.crt)

Step -7:- We can go to Directory when store Certificate and select PRITHVIRAJ.crt and show details of Certificate.



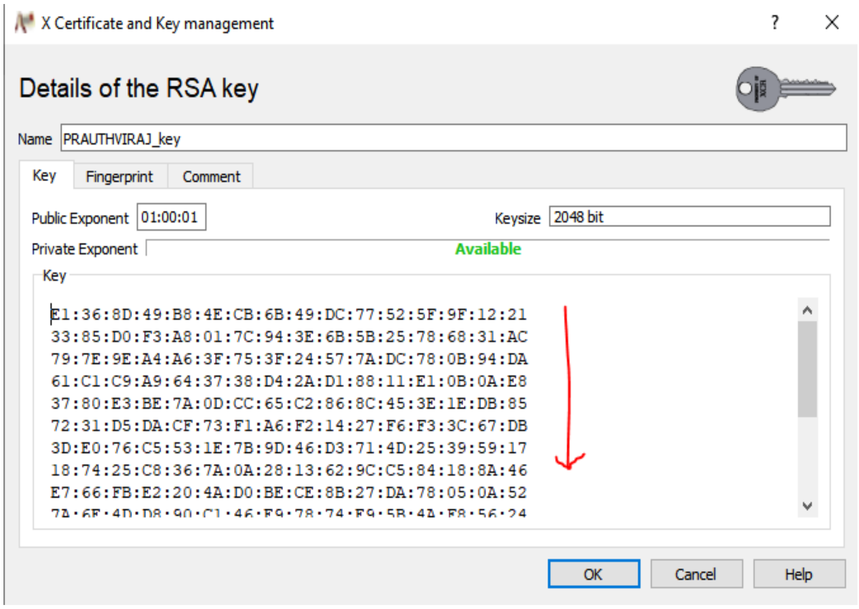
Details of the Certificate

Internal name: PRITHVI
Signature: Signer unknown | sha256WithRSAEncryption
Key: Show public key
Serial: 6DAD0A1C8DEA025B

Fingerprints
MD5: 9B:CE:68:7E:3D:27:97:66:8A:37:77:3A:72:3E:15:EB
SHA1: C5:45:E4:35:BC:B0:67:16:3E:74:B7:B7:06:D8:85:DC:2D:BB:1B:91
SHA256: CB:A9:FB:DA:7D:13:E8:12:E9:88:E9:E5:98:B2:A6:1C
66:6D:5E:20:E1:A0:2C:F4:C4:B3:F4:83:A0:62:CC:5E

Validity
16 September, 2022 4:10:00 PM | 16 September, 2023 4:10:00 PM | Valid

Now we can select Subject that show RSA Key



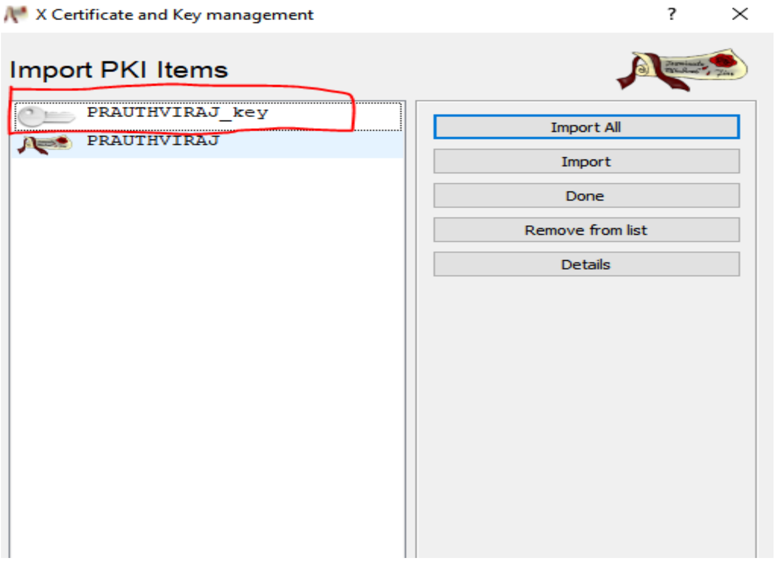
Details of the RSA key

Name: PRAUTHVIRAJ_key

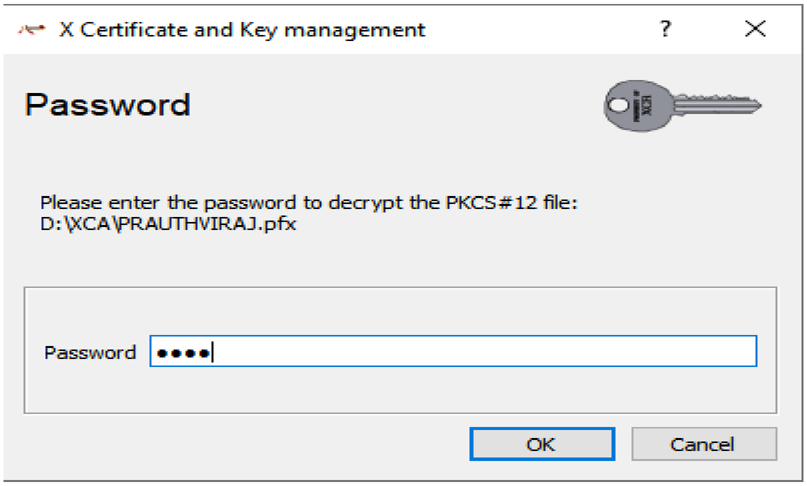
Public Exponent: 01:00:01
Keysize: 2048 bit
Private Exponent: Available

Key
```
E1:36:8D:49:B8:4E:CB:6B:49:DC:77:52:5F:9F:12:21
33:85:D0:F3:A8:01:7C:94:3E:6B:5B:25:78:68:31:AC
79:7E:9E:A4:A6:3F:75:3F:24:57:7A:DC:78:0B:94:DA
61:C1:C9:A9:64:37:38:D4:2A:D1:88:11:E1:0B:0A:E8
37:80:E3:BE:7A:0D:CC:65:C2:86:8C:45:3E:1E:DB:85
72:31:D5:DA:CF:73:F1:A6:F2:14:27:F6:F3:3C:67:DB
3D:E0:76:C5:53:1E:7B:9D:46:D3:71:4D:25:39:59:17
18:74:25:C8:36:7A:0A:28:13:62:9C:C5:84:18:8A:46
E7:66:FB:E2:20:4A:D0:BE:CE:8B:27:DA:78:05:0A:52
7A:6F:4D:D8:90:C1:46:F9:78:74:F9:5B:4A:F8:56:24
```

Step -8:- Now we can select PRITHVIRAJ.pfx and Select PRITHVIRAJ_KEY option and Click it.



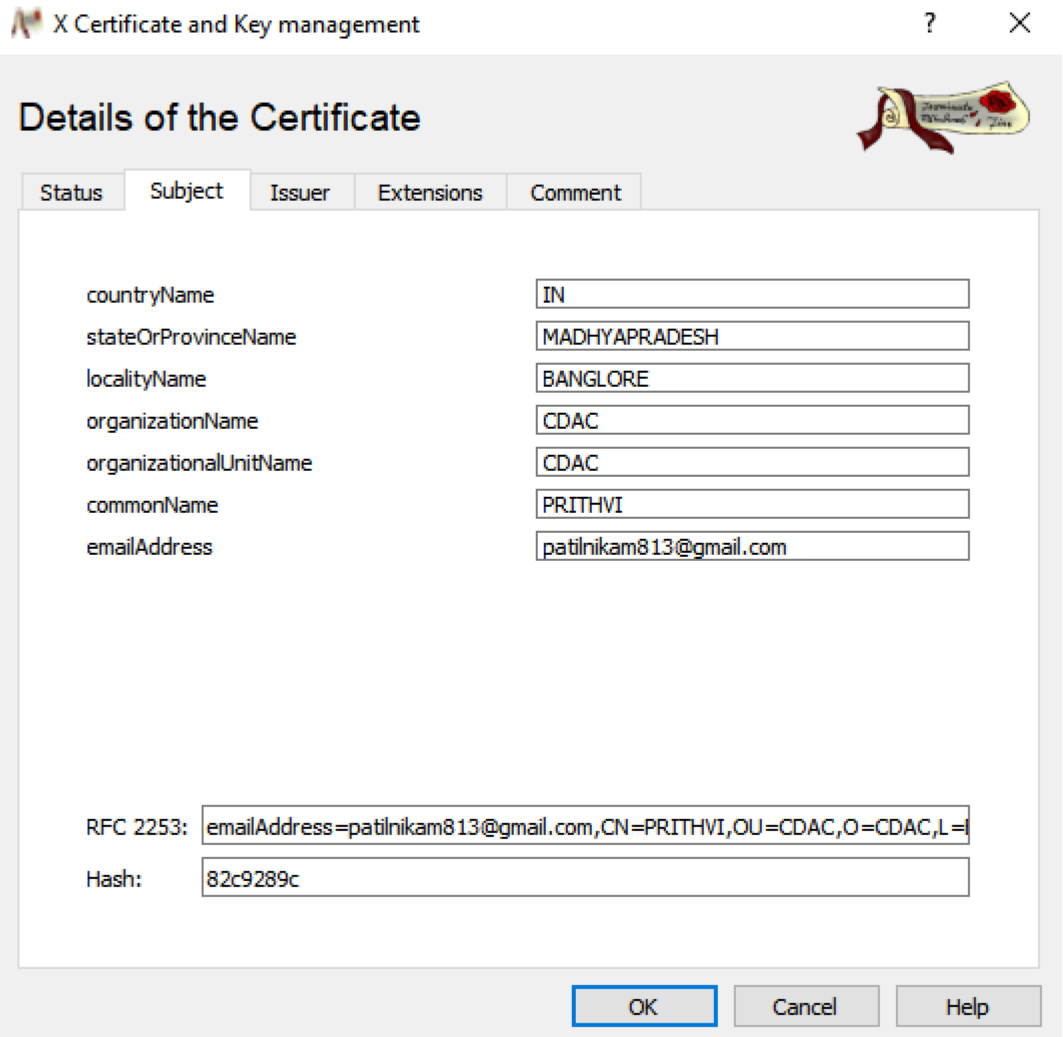
After Clicking on PRITHVIRAJ_key open new popup that show password Enter option and put password on it.



Please enter the password to decrypt the PKCS#12 file:
D:\XCA\PRAUTHVIRAJ.pfx

Password ••••

Now Open new window that show Certificate Details.



countryName	IN
stateOrProvinceName	MADHYAPRADESH
localityName	BANGLORE
organizationName	CDAC
organizationalUnitName	CDAC
commonName	PRITHVI
emailAddress	patilnikam813@gmail.com

RFC 2253: emailAddress=patilnikam813@gmail.com,CN=PRITHVI,OU=CDAC,O=CDAC,L=I

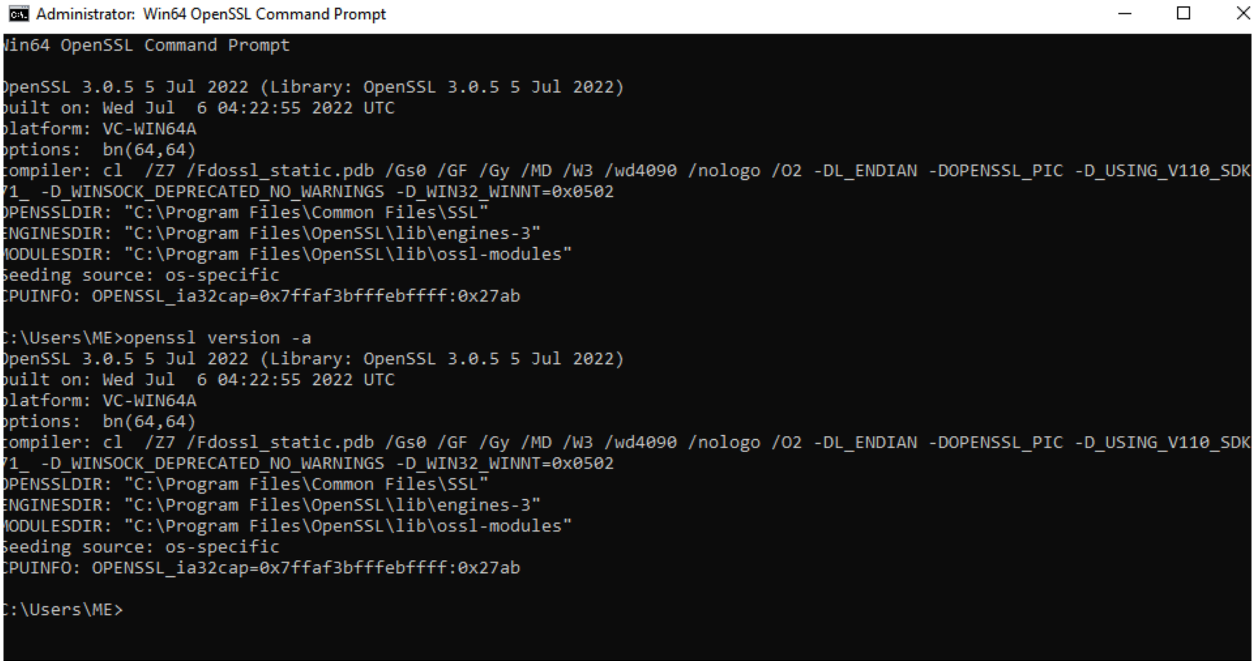
Hash: 82c9289c

OPEN SSL:-

PRACTICAL :- Digital Signature Certificate (DSC)

Step – 1:- To check the version of openssl

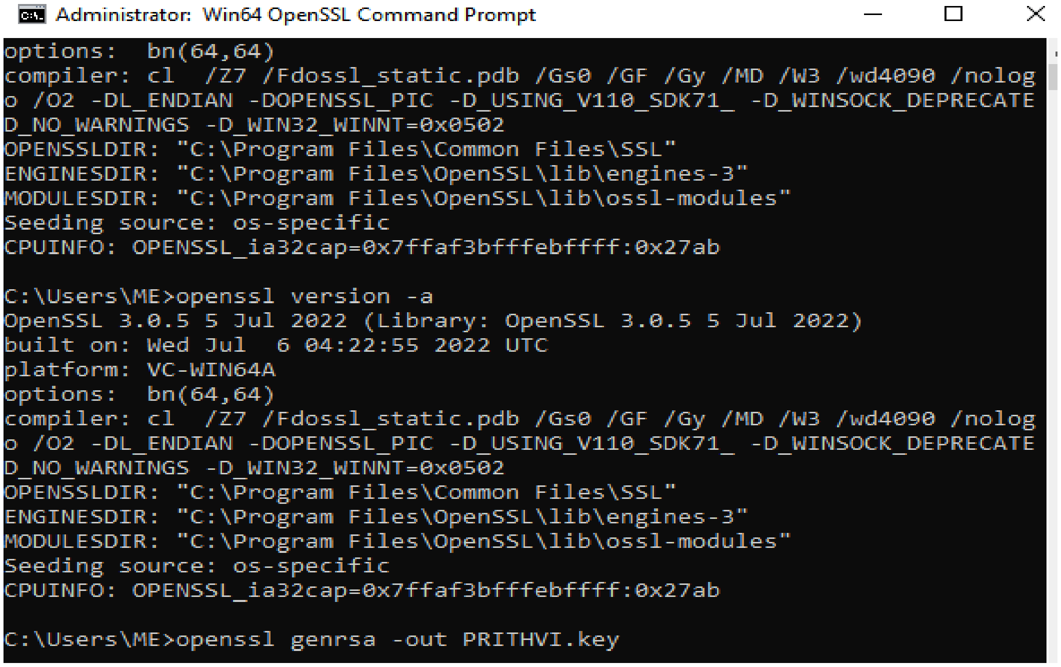
Command:- openssl versio –a



```
Jin64 OpenSSL Command Prompt

OpenSSL 3.0.5 5 Jul 2022 (Library: OpenSSL 3.0.5 5 Jul 2022)
ouilt on: Wed Jul  6 04:22:55 2022 UTC
olatform: VC-WIN64A
options:  bn(64,64)
compiler: cl  /Z7 /Fdossl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nologo /O2 -DL_ENDIAN -DOPENSSL_PIC -D_USING_V110_SDK
71_ -D_WINSOCK_DEPRECATED_NO_WARNINGS -D_WIN32_WINNT=0x0502
OPENSSLDIR: "C:\Program Files\Common Files\SSL"
ENGINESDIR: "C:\Program Files\OpenSSL\lib\engines-3"
MODULESDIR: "C:\Program Files\OpenSSL\lib\ossl-modules"
Seeding source: os-specific
CPUINFO: OPENSSL_ia32cap=0x7ffaf3bfffebffff:0x27ab

:\Users\ME>openssl version -a
OpenSSL 3.0.5 5 Jul 2022 (Library: OpenSSL 3.0.5 5 Jul 2022)
ouilt on: Wed Jul  6 04:22:55 2022 UTC
olatform: VC-WIN64A
options:  bn(64,64)
compiler: cl  /Z7 /Fdossl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nologo /O2 -DL_ENDIAN -DOPENSSL_PIC -D_USING_V110_SDK
71_ -D_WINSOCK_DEPRECATED_NO_WARNINGS -D_WIN32_WINNT=0x0502
OPENSSLDIR: "C:\Program Files\Common Files\SSL"
ENGINESDIR: "C:\Program Files\OpenSSL\lib\engines-3"
MODULESDIR: "C:\Program Files\OpenSSL\lib\ossl-modules"
Seeding source: os-specific
CPUINFO: OPENSSL_ia32cap=0x7ffaf3bfffebffff:0x27ab

:\Users\ME>
```

Step- 2 :- To Generate key pair:-

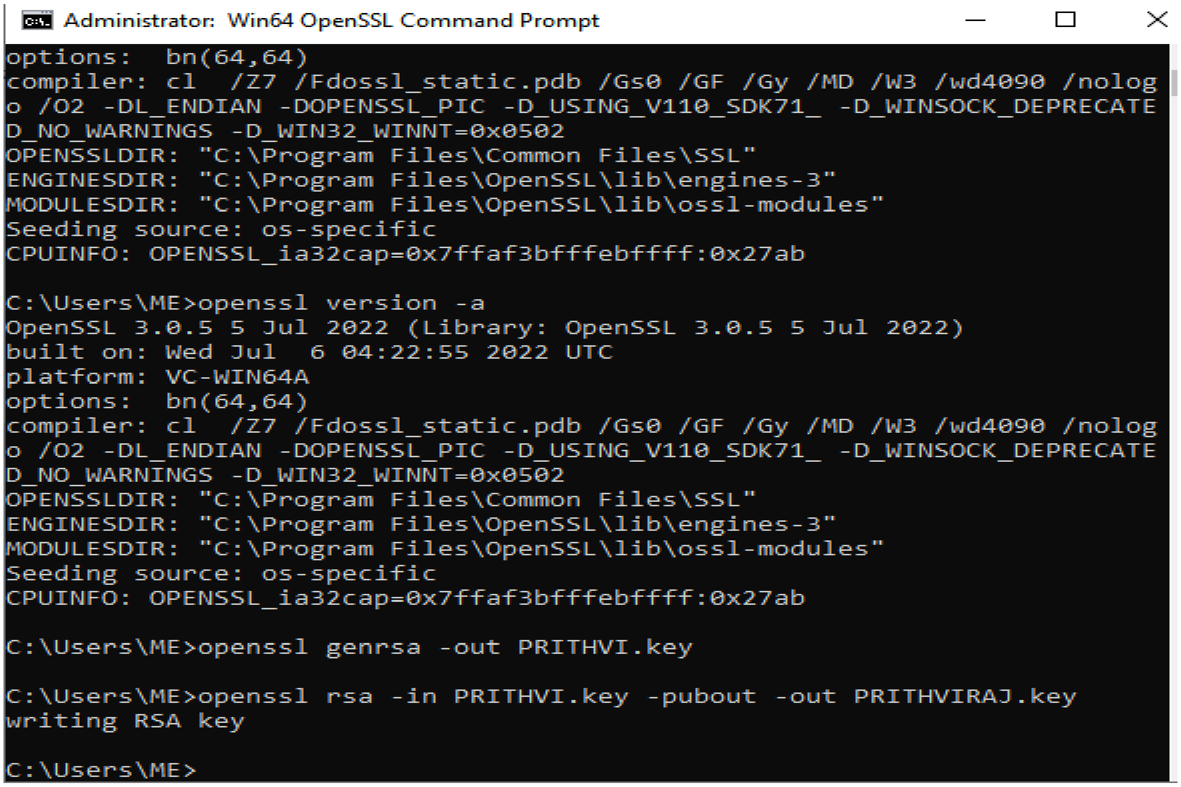
Command:- openssl genrsa -out name_of_your_file_cont_thekeypair.key



```
options:  bn(64,64)
compiler: cl  /Z7 /Fdossl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nolog
o /O2 -DL_ENDIAN -DOPENSSL_PIC -D_USING_V110_SDK71_ -D_WINSOCK_DEPRECATE
D_NO_WARNINGS -D_WIN32_WINNT=0x0502
OPENSSLDIR: "C:\Program Files\Common Files\SSL"
ENGINESDIR: "C:\Program Files\OpenSSL\lib\engines-3"
MODULESDIR: "C:\Program Files\OpenSSL\lib\ossl-modules"
Seeding source: os-specific
CPUINFO: OPENSSL_ia32cap=0x7ffaf3bfffebffff:0x27ab

C:\Users\ME>openssl version -a
OpenSSL 3.0.5 5 Jul 2022 (Library: OpenSSL 3.0.5 5 Jul 2022)
built on: Wed Jul  6 04:22:55 2022 UTC
platform: VC-WIN64A
options:  bn(64,64)
compiler: cl  /Z7 /Fdossl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nolog
o /O2 -DL_ENDIAN -DOPENSSL_PIC -D_USING_V110_SDK71_ -D_WINSOCK_DEPRECATE
D_NO_WARNINGS -D_WIN32_WINNT=0x0502
OPENSSLDIR: "C:\Program Files\Common Files\SSL"
ENGINESDIR: "C:\Program Files\OpenSSL\lib\engines-3"
MODULESDIR: "C:\Program Files\OpenSSL\lib\ossl-modules"
Seeding source: os-specific
CPUINFO: OPENSSL_ia32cap=0x7ffaf3bfffebffff:0x27ab

C:\Users\ME>openssl genrsa -out PRITHVI.key
```

Step- 3:- To Extract the public key form the key pair file:

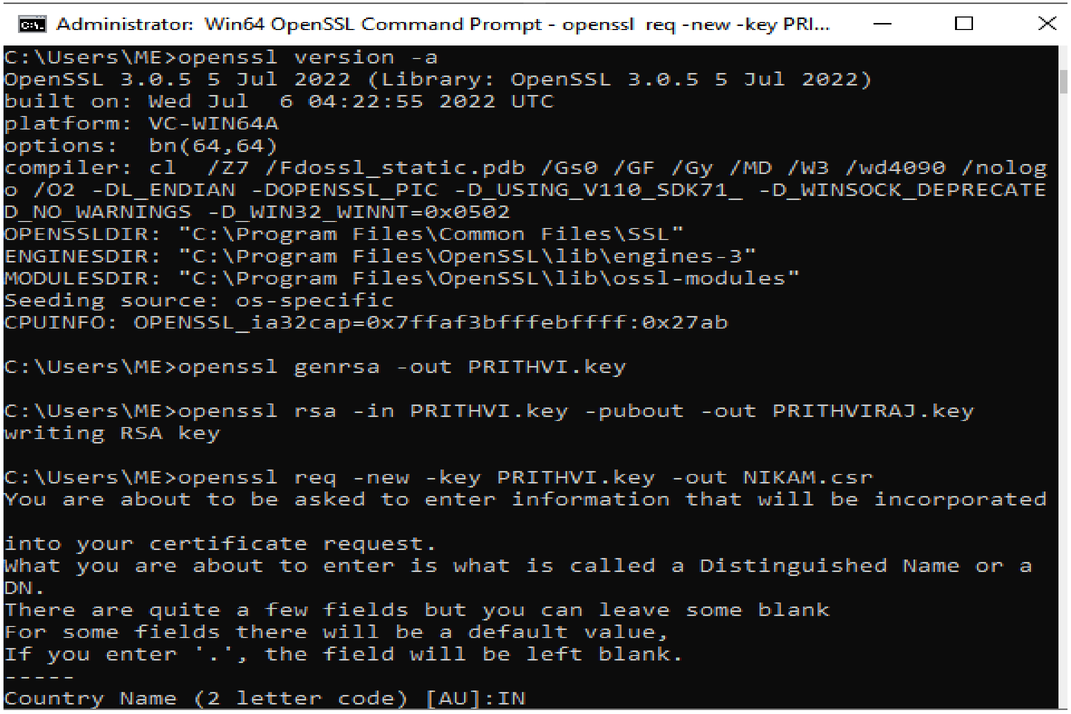
Command :- openssl rsa -in name_of_your_file_cont_thekeypair.key -pubout -out public_key_file.key



```
options:  bn(64,64)
compiler: cl  /Z7 /Fdossl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nolog
o /O2 -DL_ENDIAN -DOPENSSL_PIC -D_USING_V110_SDK71_ -D_WINSOCK_DEPRECATE
D_NO_WARNINGS -D_WIN32_WINNT=0x0502
OPENSSLDIR: "C:\Program Files\Common Files\SSL"
ENGINESDIR: "C:\Program Files\OpenSSL\lib\engines-3"
MODULESDIR: "C:\Program Files\OpenSSL\lib\ossl-modules"
Seeding source: os-specific
CPUINFO: OPENSSL_ia32cap=0x7ffaf3bfffebffff:0x27ab

C:\Users\ME>openssl version -a
OpenSSL 3.0.5 5 Jul 2022 (Library: OpenSSL 3.0.5 5 Jul 2022)
built on: Wed Jul  6 04:22:55 2022 UTC
platform: VC-WIN64A
options:  bn(64,64)
compiler: cl  /Z7 /Fdossl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nolog
o /O2 -DL_ENDIAN -DOPENSSL_PIC -D_USING_V110_SDK71_ -D_WINSOCK_DEPRECATE
D_NO_WARNINGS -D_WIN32_WINNT=0x0502
OPENSSLDIR: "C:\Program Files\Common Files\SSL"
ENGINESDIR: "C:\Program Files\OpenSSL\lib\engines-3"
MODULESDIR: "C:\Program Files\OpenSSL\lib\ossl-modules"
Seeding source: os-specific
CPUINFO: OPENSSL_ia32cap=0x7ffaf3bfffebffff:0x27ab

C:\Users\ME>openssl genrsa -out PRITHVI.key

C:\Users\ME>openssl rsa -in PRITHVI.key -pubout -out PRITHVIRAJ.key
writing RSA key

C:\Users\ME>
```

Step- 4:- To Create certificate signing request:-

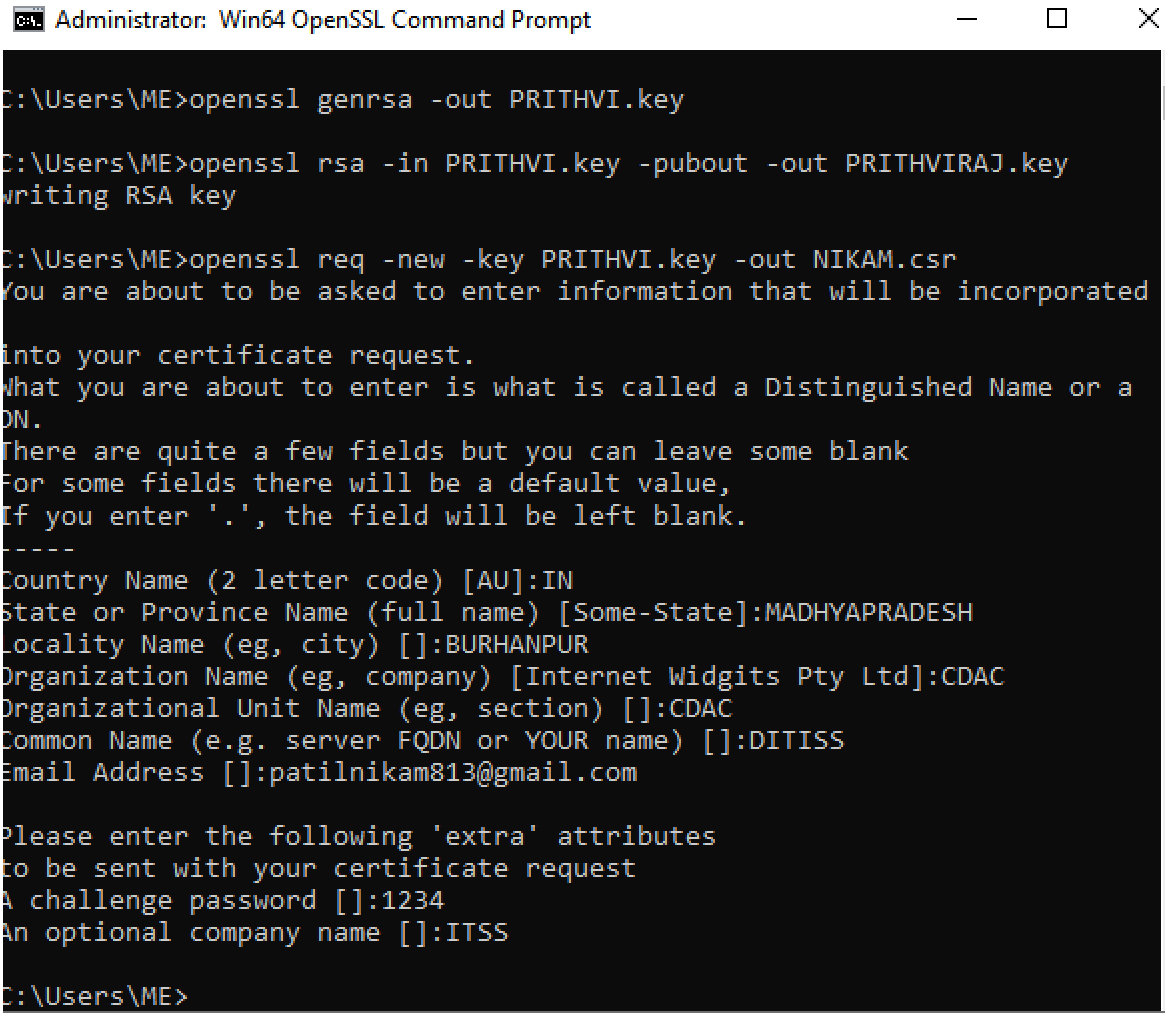
Command:- openssl req -new -key name_of_your_file_cont_thekeypair.key –out name_of_the_csr_file.csr


Administrator: Win64 OpenSSL Command Prompt - openssl req -new -key PRI...

```
C:\Users\ME>openssl version -a
OpenSSL 3.0.5 5 Jul 2022 (Library: OpenSSL 3.0.5 5 Jul 2022)
built on: Wed Jul  6 04:22:55 2022 UTC
platform: VC-WIN64A
options:  bn(64,64)
compiler: cl  /Z7 /Fdossl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nolog
o /O2 -DL_ENDIAN -DOPENSSL_PIC -D_USING_V110_SDK71_ -D_WINSOCK_DEPRECATE
D_NO_WARNINGS -D_WIN32_WINNT=0x0502
OPENSSLDIR: "C:\Program Files\Common Files\SSL"
ENGINESDIR: "C:\Program Files\OpenSSL\lib\engines-3"
MODULESDIR: "C:\Program Files\OpenSSL\lib\ossl-modules"
Seeding source: os-specific
CPUINFO: OPENSSL_ia32cap=0x7ffaf3bfffebffff:0x27ab

C:\Users\ME>openssl genrsa -out PRITHVI.key

C:\Users\ME>openssl rsa -in PRITHVI.key -pubout -out PRITHVIRAJ.key
writing RSA key

C:\Users\ME>openssl req -new -key PRITHVI.key -out NIKAM.csr
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
```

Step- 5:- To verify the details of csr

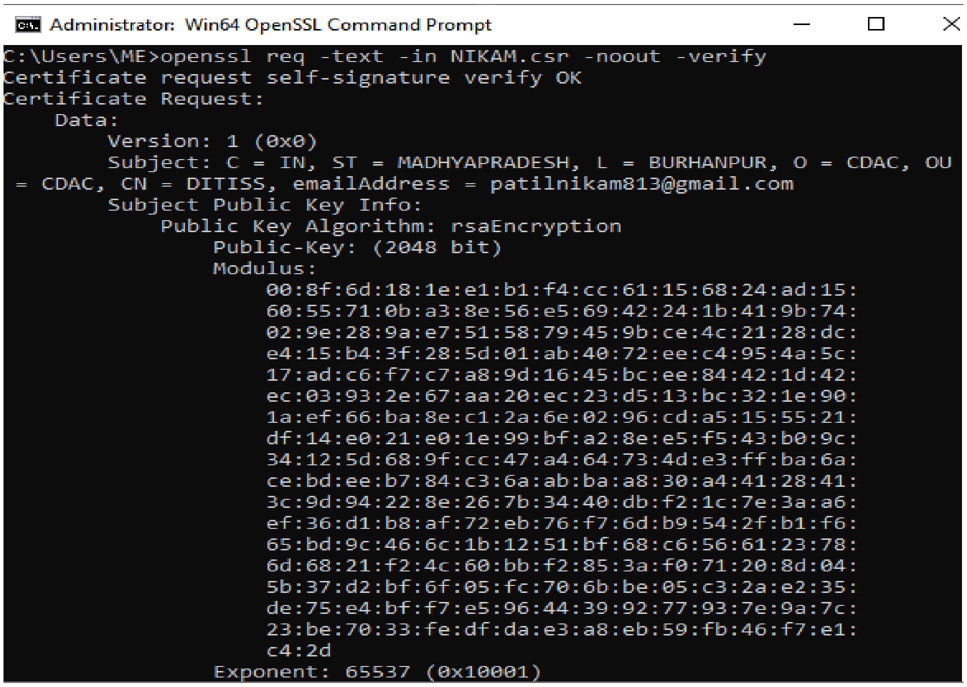
Command:- openssl req -text -in name_of_the_csr_file.csr -noout –verify



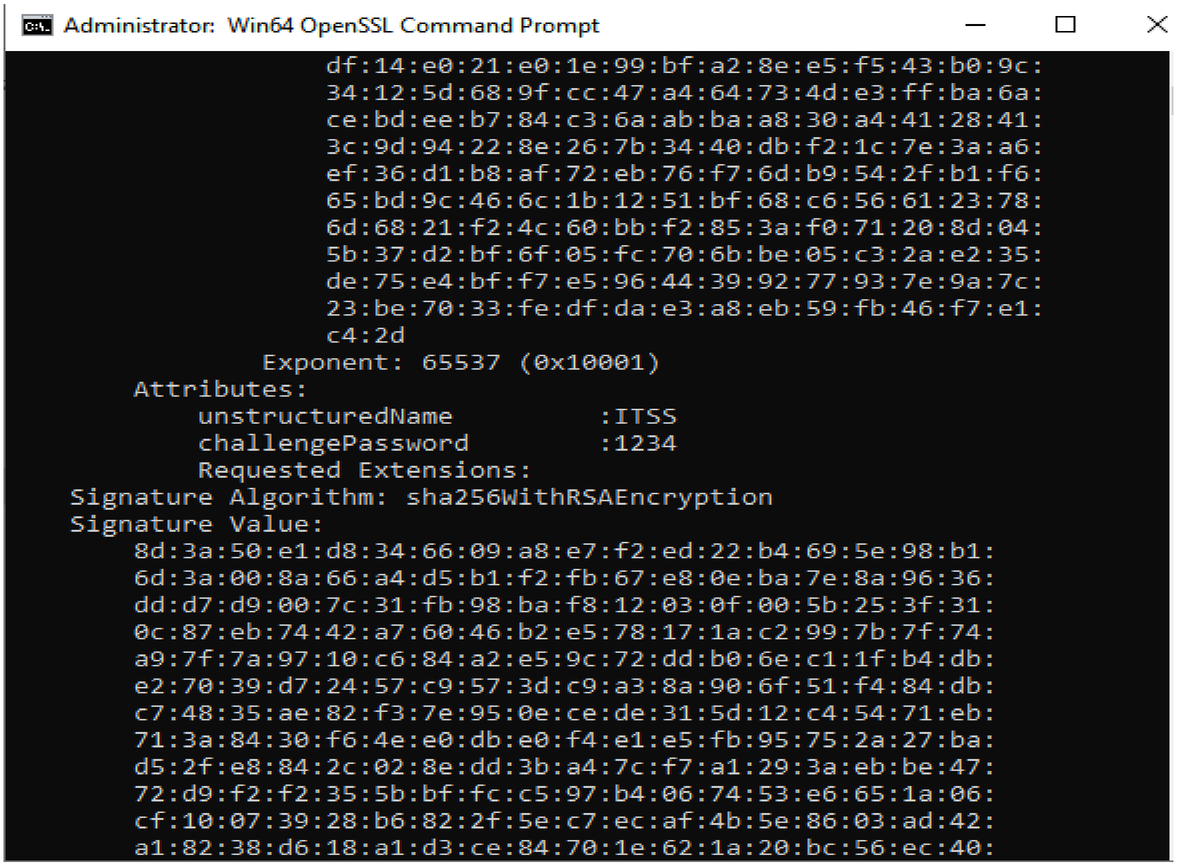
```
C:\Users\ME>openssl genrsa -out PRITHVI.key

C:\Users\ME>openssl rsa -in PRITHVI.key -pubout -out PRITHVIRAJ.key
writing RSA key

C:\Users\ME>openssl req -new -key PRITHVI.key -out NIKAM.csr
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]:MADHYAPRADESH
Locality Name (eg, city) []:BURHANPUR
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CDAC
Organizational Unit Name (eg, section) []:CDAC
Common Name (e.g. server FQDN or YOUR name) []:DITISS
Email Address []:patilnikam813@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:ITSS

C:\Users\ME>
```

Step – 6:- To Genrate the Self Sign certificate

Command:- openssl x509 -in name_of_the_csr_file.csr -out name_of_the_certificate_file.crt -req -signkey name_of_your_file_cont_thekeypair.key -days 365



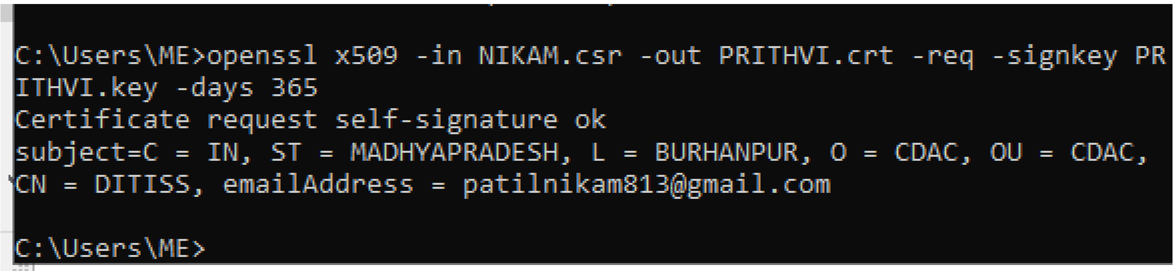
```
C:\Users\ME>openssl req -text -in NIKAM.csr -noout -verify
Certificate request self-signature verify OK
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = IN, ST = MADHYAPRADESH, L = BURHANPUR, O = CDAC, OU
 = CDAC, CN = DITISS, emailAddress = patilnikam813@gmail.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:8f:6d:18:1e:e1:b1:f4:cc:61:15:68:24:ad:15:
                    60:55:71:0b:a3:8e:56:e5:69:42:24:1b:41:9b:74:
                    02:9e:28:9a:e7:51:58:79:45:9b:ce:4c:21:28:dc:
                    e4:15:b4:3f:28:5d:01:ab:40:72:ee:c4:95:4a:5c:
                    17:ad:c6:f7:c7:a8:9d:16:45:bc:ee:84:42:1d:42:
                    ec:03:93:2e:67:aa:20:ec:23:d5:13:bc:32:1e:90:
                    1a:ef:66:ba:8e:c1:2a:6e:02:96:cd:a5:15:55:21:
                    df:14:e0:21:e0:1e:99:bf:a2:8e:e5:f5:43:b0:9c:
                    34:12:5d:68:9f:cc:47:a4:64:73:4d:e3:ff:ba:6a:
                    ce:bd:ee:b7:84:c3:6a:ab:ba:a8:30:a4:41:28:41:
                    3c:9d:94:22:8e:26:7b:34:40:db:f2:1c:7e:3a:a6:
                    ef:36:d1:b8:af:72:eb:76:f7:6d:b9:54:2f:b1:f6:
                    65:bd:9c:46:6c:1b:12:51:bf:68:c6:56:61:23:78:
                    6d:68:21:f2:4c:60:bb:f2:85:3a:f0:71:20:8d:04:
                    5b:37:d2:bf:6f:05:fc:70:6b:be:05:c3:2a:e2:35:
                    de:75:e4:bf:f7:e5:96:44:39:92:77:93:7e:9a:7c:
                    23:be:70:33:fe:df:da:e3:a8:eb:59:fb:46:f7:e1:
                    c4:2d
                Exponent: 65537 (0x10001)
```



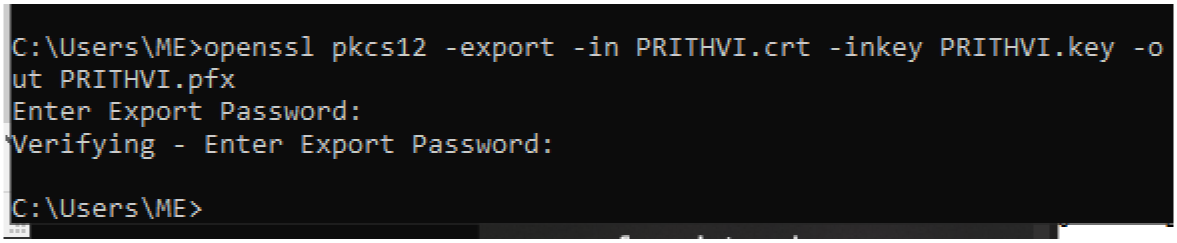
```
                    df:14:e0:21:e0:1e:99:bf:a2:8e:e5:f5:43:b0:9c:
                    34:12:5d:68:9f:cc:47:a4:64:73:4d:e3:ff:ba:6a:
                    ce:bd:ee:b7:84:c3:6a:ab:ba:a8:30:a4:41:28:41:
                    3c:9d:94:22:8e:26:7b:34:40:db:f2:1c:7e:3a:a6:
                    ef:36:d1:b8:af:72:eb:76:f7:6d:b9:54:2f:b1:f6:
                    65:bd:9c:46:6c:1b:12:51:bf:68:c6:56:61:23:78:
                    6d:68:21:f2:4c:60:bb:f2:85:3a:f0:71:20:8d:04:
                    5b:37:d2:bf:6f:05:fc:70:6b:be:05:c3:2a:e2:35:
                    de:75:e4:bf:f7:e5:96:44:39:92:77:93:7e:9a:7c:
                    23:be:70:33:fe:df:da:e3:a8:eb:59:fb:46:f7:e1:
                    c4:2d
                Exponent: 65537 (0x10001)
        Attributes:
            unstructuredName         :ITSS
            challengePassword        :1234
            Requested Extensions:
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        8d:3a:50:e1:d8:34:66:09:a8:e7:f2:ed:22:b4:69:5e:98:b1:
        6d:3a:00:8a:66:a4:d5:b1:f2:fb:67:e8:0e:ba:7e:8a:96:36:
        dd:d7:d9:00:7c:31:fb:98:ba:f8:12:03:0f:00:5b:25:3f:31:
        0c:87:eb:74:42:a7:60:46:b2:e5:78:17:1a:c2:99:7b:7f:74:
        a9:7f:7a:97:10:c6:84:a2:e5:9c:72:dd:b0:6e:c1:1f:b4:db:
        e2:70:39:d7:24:57:c9:57:3d:c9:a3:8a:90:6f:51:f4:84:db:
        c7:48:35:ae:82:f3:7e:95:0e:ce:de:31:5d:12:c4:54:71:eb:
        71:3a:84:30:f6:4e:e0:db:e0:f4:e1:e5:fb:95:75:2a:27:ba:
        d5:2f:e8:84:2c:02:8e:dd:3b:a4:7c:f7:a1:29:3a:eb:be:47:
        72:d9:f2:f2:35:5b:bf:fc:c5:97:b4:06:74:53:e6:65:1a:06:
        cf:10:07:39:28:b6:82:2f:5e:c7:ec:af:4b:5e:86:03:ad:42:
        a1:82:38:d6:18:a1:d3:ce:84:70:1e:62:1a:20:bc:56:ec:40:
```

Step- 7:- To Export the crt file into PFX file (pfx file for windows)

Command:- openssl pkcs12 -export -in akshay.crt -inkey akshay.key -out akshay.pfx

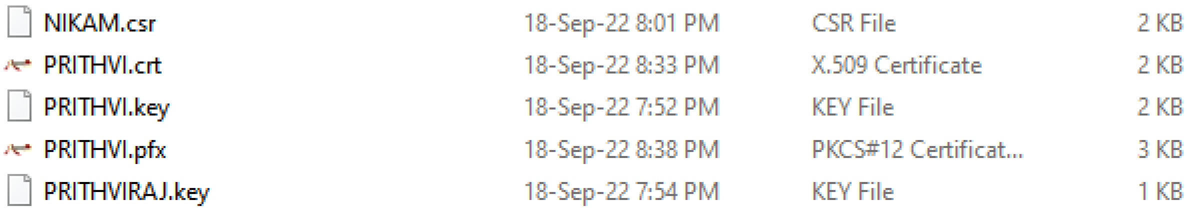


```
C:\Users\ME>openssl x509 -in NIKAM.csr -out PRITHVI.crt -req -signkey PR
ITHVI.key -days 365
Certificate request self-signature ok
subject=C = IN, ST = MADHYAPRADESH, L = BURHANPUR, O = CDAC, OU = CDAC,
CN = DITISS, emailAddress = patilnikam813@gmail.com

C:\Users\ME>
```

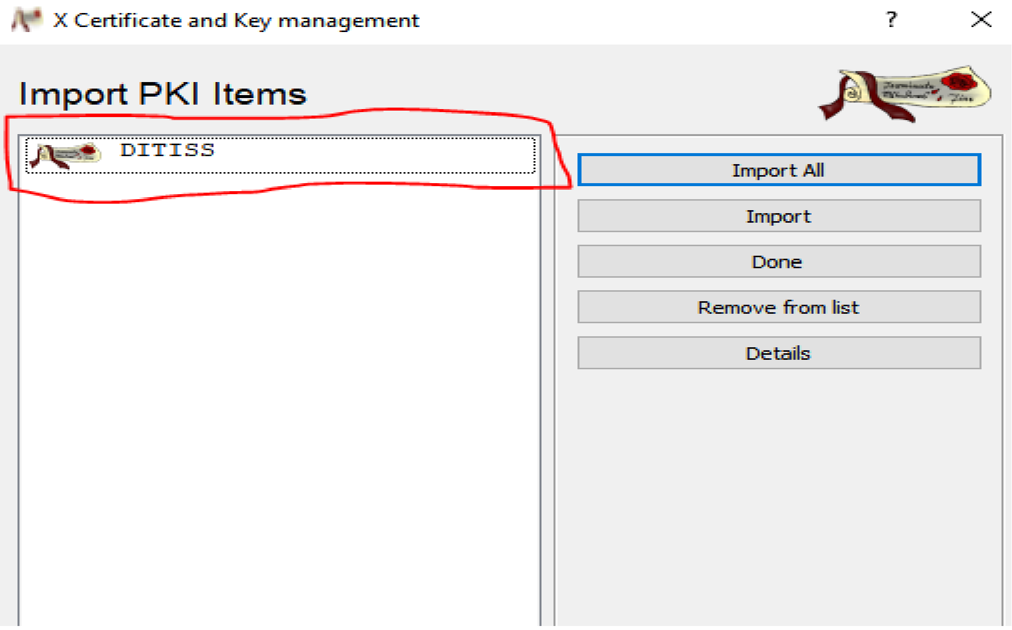


```
C:\Users\ME>openssl pkcs12 -export -in PRITHVI.crt -inkey PRITHVI.key -o
ut PRITHVI.pfx
Enter Export Password:
Verifying - Enter Export Password:

C:\Users\ME>
```

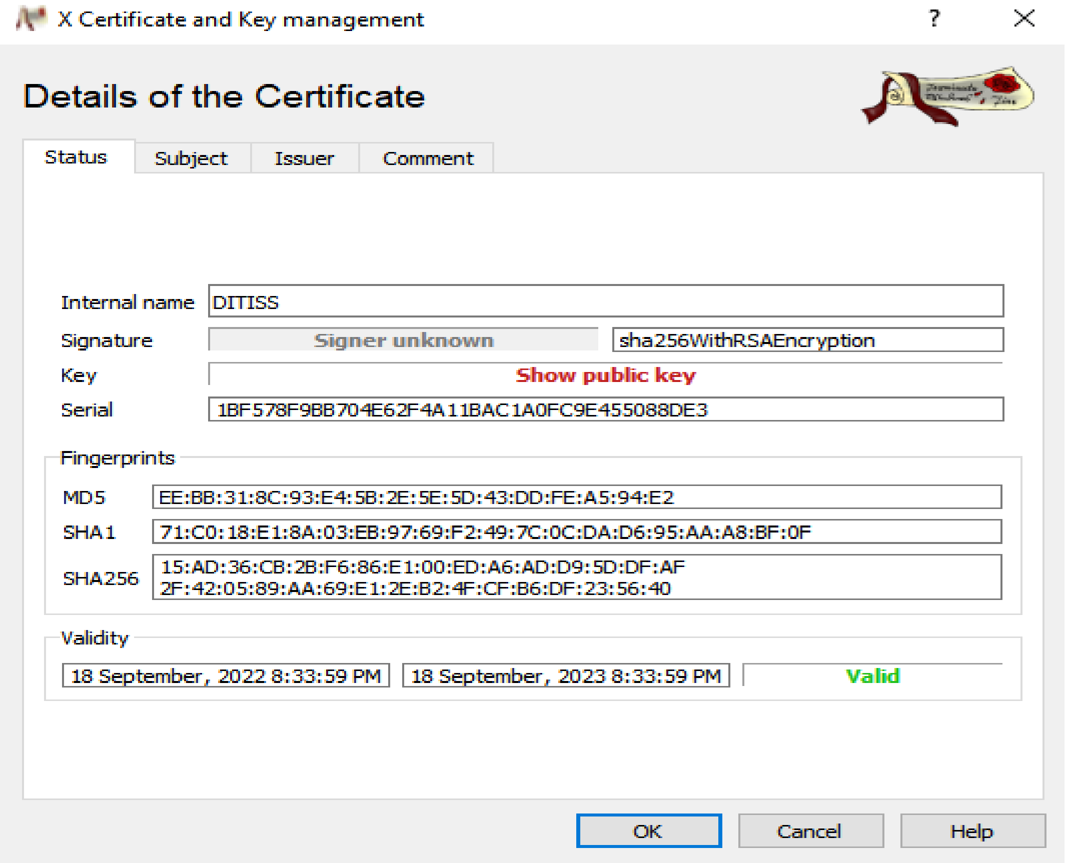
Step-8:- We can go to Directory when store Certificate and select PRITHVIRAJ.crt and show details of Certificate.



NIKAM.csr	18-Sep-22 8:01 PM	CSR File	2 KB
PRITHVI.crt	18-Sep-22 8:33 PM	X.509 Certificate	2 KB
PRITHVI.key	18-Sep-22 7:52 PM	KEY File	2 KB
PRITHVI.pfx	18-Sep-22 8:38 PM	PKCS#12 Certificat...	3 KB
PRITHVIRAJ.key	18-Sep-22 7:54 PM	KEY File	1 KB



Now we can Show the detail of Certificate



Internal name DITISS

Signature Signer unknown sha256WithRSAEncryption

Key

Serial 1BF578F9BB704E62F4A11BAC1A0FC9E455088DE3

Fingerprints

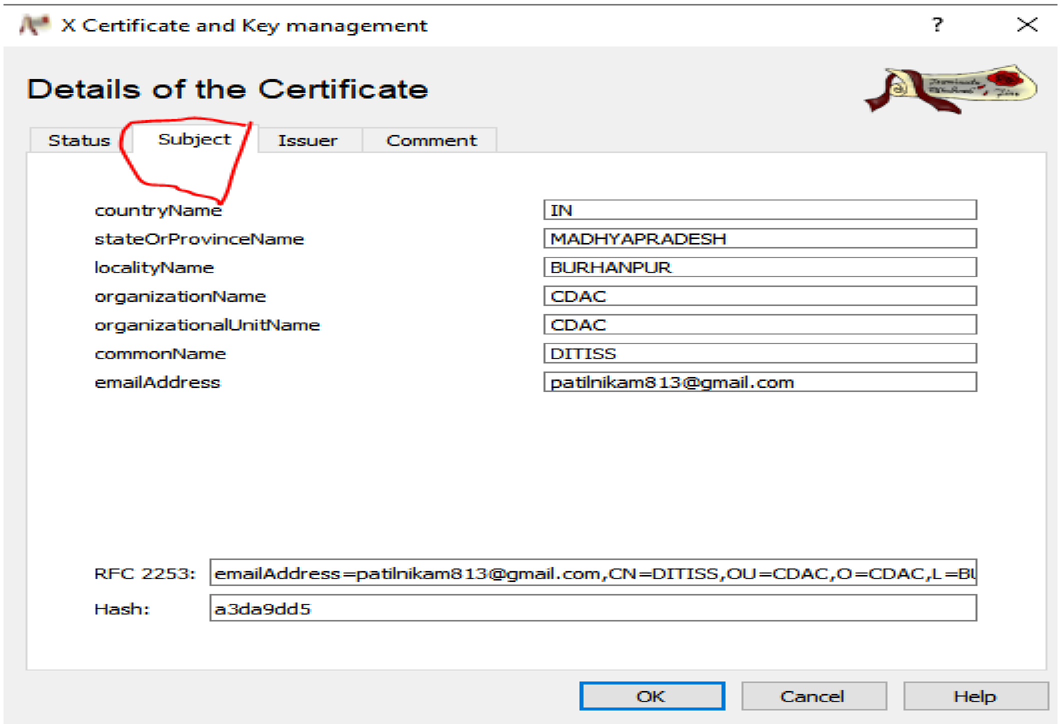
MD5 EE:BB:31:8C:93:E4:5B:2E:5E:5D:43:DD:FE:A5:94:E2

SHA1 71:C0:18:E1:8A:03:EB:97:69:F2:49:7C:0C:DA:D6:95:AA:A8:BF:0F

SHA256 15:AD:36:CB:2B:F6:86:E1:00:ED:A6:AD:D9:5D:DF:AF
2F:42:05:89:AA:69:E1:2E:B2:4F:CF:B6:DF:23:56:40

Validity

18 September, 2022 8:33:59 PM 18 September, 2023 8:33:59 PM Valid

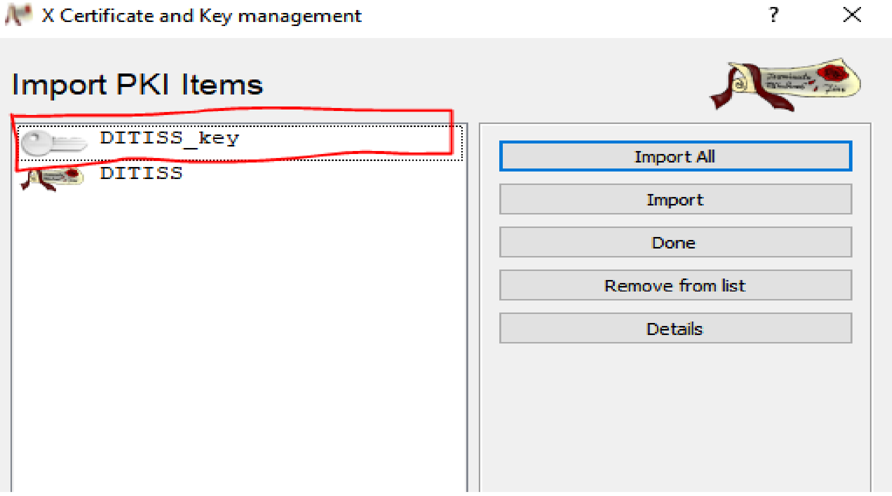


countryName IN
stateOrProvinceName MADHYAPRADESH
localityName BURHANPUR
organizationName CDAC
organizationalUnitName CDAC
commonName DITISS
emailAddress patilnikam813@gmail.com

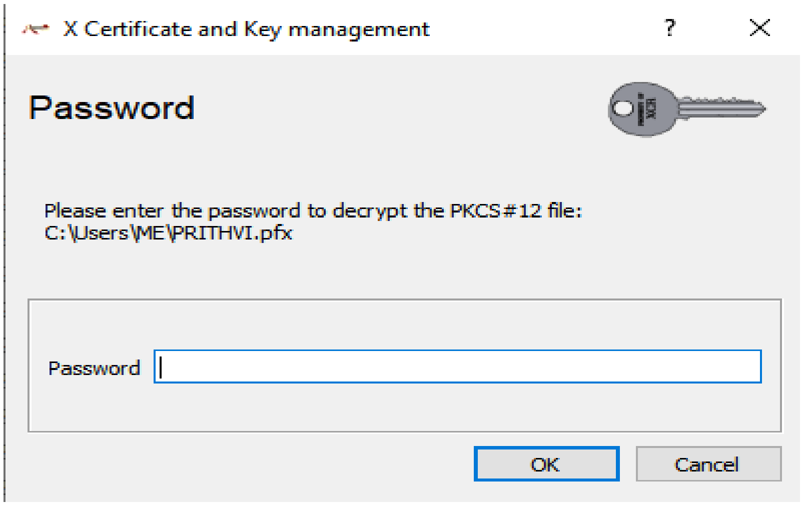
RFC 2253: emailAddress=patilnikam813@gmail.com,CN=DITISS,OU=CDAC,O=CDAC,L=B

Hash: a3da9dd5

Step -10:- Now we can select PRITHVIRAJ.pfx and Select PRITHVIRAJ_KEY option and Click it.



Now Put Password(****)

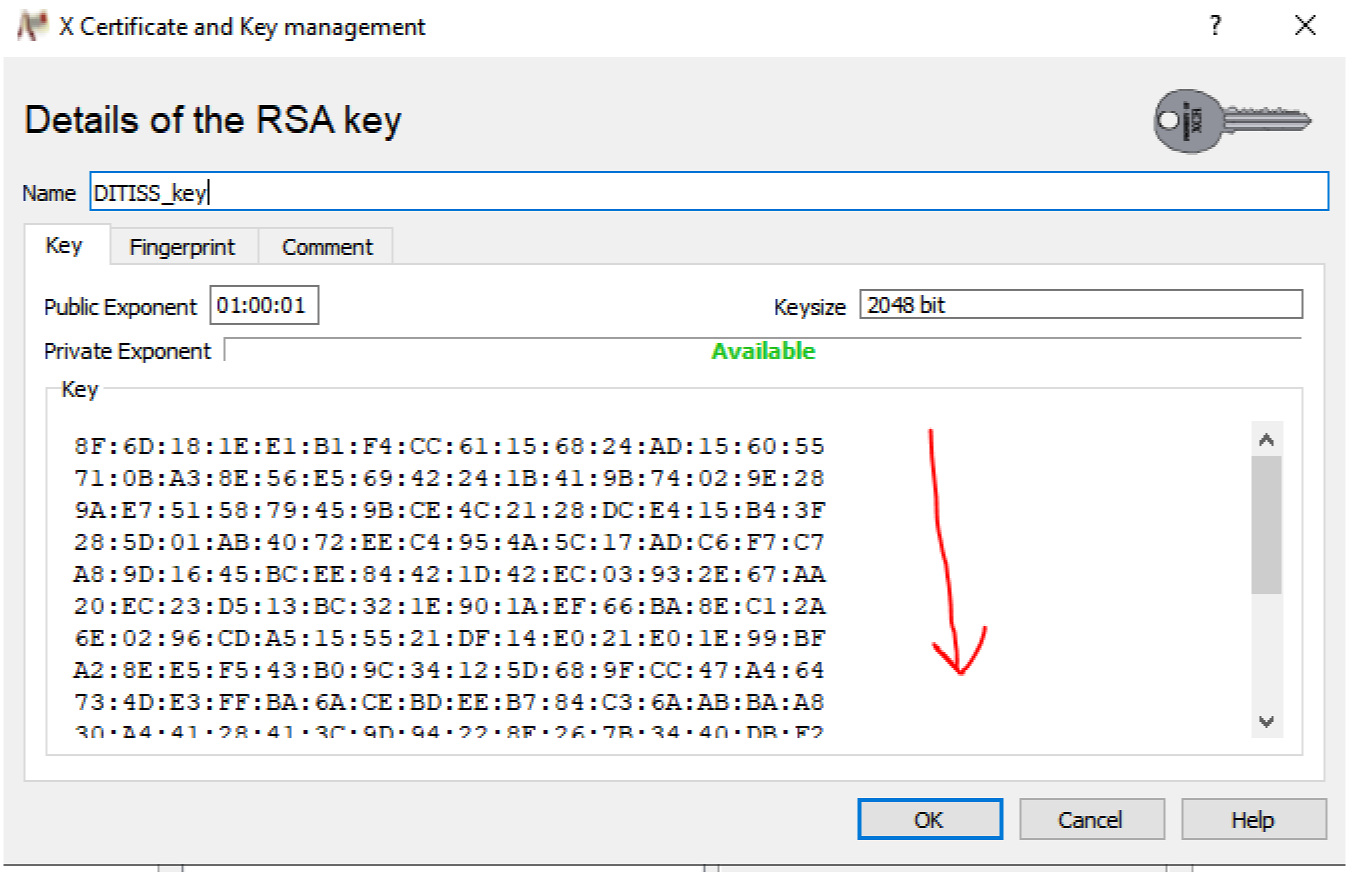


Password

Please enter the password to decrypt the PKCS#12 file:
C:\Users\ME\PRITHVI.pfx

Password |

After Clicking on DITISS_key open new popup that show password Enter option and put password on it.



Details of the RSA key

Name DITISS_key

Public Exponent 01:00:01

Keysize 2048 bit

Private Exponent Available

Key

```
8F:6D:18:1E:E1:B1:F4:CC:61:15:68:24:AD:15:60:55
71:0B:A3:8E:56:E5:69:42:24:1B:41:9B:74:02:9E:28
9A:E7:51:58:79:45:9B:CE:4C:21:28:DC:E4:15:B4:3F
28:5D:01:AB:40:72:EE:C4:95:4A:5C:17:AD:C6:F7:C7
A8:9D:16:45:BC:EE:84:42:1D:42:EC:03:93:2E:67:AA
20:EC:23:D5:13:BC:32:1E:90:1A:EF:66:BA:8E:C1:2A
6E:02:96:CD:A5:15:55:21:DF:14:E0:21:E0:1E:99:BF
A2:8E:E5:F5:43:B0:9C:34:12:5D:68:9F:CC:47:A4:64
73:4D:E3:FF:BA:6A:CE:BD:EE:B7:84:C3:6A:AB:BA:A8
30:A4:41:28:41:3C:9D:94:22:8F:26:7B:34:40:DB:F2
```