OpenSSL --- E-Mail Signing

The complete list of OpenSSL commands (incl. Arguments) that were used to generate the private key and certificate are:

#Commands used in creating directories needed by *OpenSSl sudo -s mkdir*
openssl chmod 700 openssl cd openssl cp /usr/lib/ssl/openssl.cnf .
&& mkdir demoCA chmod 700
demoCA
cd demoCA
mkdir {newcerts,crl,certs$(touch {index.txt,serial})} echo 1000 >serial

#Commands used in creating certificate and private keys

openssl req -new -x509 -days 365 -keyout ca.key -out ca.crt -config openssl.cnf openssl dsaparam 1024 >servkeyparam.pem openssl gendsa servkeyparam.pem > serv.pem
openssl req -new -key serv.pem -out server.csr -config openssl.cnf
openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf openssl pkcs12 -inkey serv.pem -in server.crt -export -out certificatehud. p12

Steps taken to import the private key and certificate into my email client(Thunderbird)

1.I opened the **Thunderbird email client**.

2.Navigated to the toolbar and selected '**Edit**'.

3.I then scrolled down to access the '**Preferences**' option which opened the Thunderbird preferences dialog box.

4.Under the '**Advanced**' option tab i selected the '**Certificates**' option and clicked on the **'View certificates**' button which popped open the certificate manager box.

5.A series of options were displayed on the tabs, I went to the '**Authorities**' option and clicked on '**Import**' to dialog box which enables one to select the file containing the certificate(CA).

6.I browsed through my directories, selected the CA, checked all three boxes that appeared, I and confirmed to proceed.

7.After confirmation, at the same certificate manager window, I choose the option '**Your certificates**', a window popped up, i browsed through my directories again and selected my '**PKCS12**' file (my certificate), Enter password and confirm.

OpenSSL print of Certificate:

openssl x509 -in 1000.pem -text -noout

Version: 3 (0x2)
Serial Number: 4096 (0x1000)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=UK, ST=SURREY, L=GUILDFORD, O=COMPUTER SCIENCE, OU=INFORMATION SECURITY, CN=NETWORK SECURITY/emailAddress=INFOSECCA@SURREY.AC.UK
Validity
Not Before: Jan 3 18:12:34 2017 GMT
Not After : Jan 3 18:12:34 2018 GMT
Subject: C=UK, ST=SURREY, O=COMPUTER SCIENCE, OU=INFORMATION SECURITY, CN=NETWORK SECURITY/emailAddress=hd00240@surrey.ac.uk
Subject Public Key Info:
Public Key Algorithm: dsaEncryption pub:
35:06:f9:26:6b:26:8c:6d:5d:80:83:2d:ac:0b:be: db:d2:f9:1d:71:50:b2:18:51:0a:c0:67:5e:9d:ba: 43:d7:a4:cd:86:8f:9b:92:b4:86:0b:05:95:50:c5:
16:0e:4e:e6:99:ce:02:e0:ed:2f:cb:66:45:84:0e: c2:0e:1d:ef:15:78:13:19:25:3d:25:cd:37:bc:90: ec:99:bc:68:ff:de:6f:e2:fb:00:c8:d3:05:de:1f:
01:f3:6a:62:4f:9e:b7:55:90:9d:10:0f:ec:a5:ff: 52:1a:04:d1:48:4b:c5:9c:eb:66:57:37:82:77:cc: db:19:58:26:05:9d:6a:0f
P:
00:bd:f4:2a:5d:e5:ff:3e:4f:65:9d:8f:31:c6:1e:
2d:93:33:59:39:a7:f2:fd:80:1b:37:e8:2d:8d:8c:
90:14:f9:c2:c4:2a:ca:3d:b9:23:fa:17:5c:1c:fb: f8:4d:5b:e0:1f:8a:10:5b:74:47:d6:3b:cc:bf:b2:
43:78:14:52:53:87:e3:a3:47:f1:2b:db:44:f2:2d: 55:91:3c:55:35:dd:9b:ce:82:27:96:97:53:70:c8: c4:fc:b6:38:c8:89:71:bf:e9:04:03:de:04:bb:bc: 1a:68:40:61:27:61:8c:50:79:ac:91:03:71:ae:5c:
3d:8f:6c:2f:43:46:66:b8:b9
Q:
00:a7:f3:d9:4a:8c:e2:08:ef:3d:51:7f:e5:dd:fe:
61:ae:8d:09:1b:1b G:
00:b2:b4:08:20:4e:f8:6f:e2:f5:fe:4b:49:b7:88:
7e:30:1e:12:41:60:5a:7d:20:86:14:ef:d7:7e:c9: 44:70:75:0e:a3:eb:86:76:75:dc:f8:bc:6d:11:40: a6:3b:53:2a:fa:b1:3d:17:e8:6a:be:3a:70:4b:2e: 95:6b:92:88:2d:86:0f:37:0c:e2:50:02:9f:e3:d7: 1e:a7:1a:7e:24:6c:f6:28:a8:4e:ba:5a:8d:a0:00: fc:39:a8:e2:a3:51:75:43:f2:5a:0a:e6:cd:80:dd: a7:66:a0:a8:56:10:da:8a:00:4c:01:bb:db:e6:b4: 6c:5b:c5:5b:ea:17:be:68:9d X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate X509v3 Subject Key Identifier:
A8:90:CD:24:51:AA:D7:F4:2C:95:1F:5F:88:B8:91:EE:50:F1:E7:94 X509v3 Authority Key Identifier:
keyid:EE:6B:C9:95:70:9E:91:E7:E0:7E:F6:F5:9F:8D:6F:AC:F6:19:49:E6

Signature Algorithm: sha256WithRSAEncryption
7b:26:2f:55:b5:f0:19:f2:fc:6a:ae:84:44:6c:c5:32:15:6a:
60:80:9f:b7:5c:17:f9:a2:a5:3c:2c:f7:ff:46:fb:7a:59:36: e2:07:e9:c9:be:d4:13:c7:1a:2a:e5:e6:58:6c:98:ea:16:b9: de:8f:1a:cc:f6:ca:6e:91:e0:60:5e:b2:ce:10:b3:81:e5:b4:
55:21:fc:17:02:d4:64:43:0e:70:46:31:49:16:b8:80:31:f0:
2e:d6:10:e0:a8:ce:b2:b1:f1:c3:f9:75:8e:92:89:c4:d4:54:
5c:20:3b:fe:88:00:70:f4:53:a1:cc:a9:5b:ac:ec:de:6e:ae:
25:91:d9:39:9a:17:35:91:ec:31:0a:10:c6:f6:83:c5:e3:95:
5a:87:92:44:a2:fb:7e:38:59:bd:a5:f4:22:a2:02:f0:08:ce:

6c:0d:77:3d:fb:7d:ce:6a:30:b9:08:6d:3f:cb:a1:fd:df:db:b0:9a:06:d9:15:b5:59:88:0c:f9:93:26:57:0d:30:0f:30:31:30:11:88:aa:20:82:3d:e0:e8:f8:80:1c:30:1c:41:a3:22:50:49:5d:91:06

5e:8f:b6:5a:0f:d6:01:cd:96:9d:46:6e:39:26:32:78:e5:57:be:8c:fd:06:32:58:79:1b:80:d2:45:cf:72:0b:bf:b1:01:fe: