Data Protection 2022

Certificate Analysis

Answer the following questions:

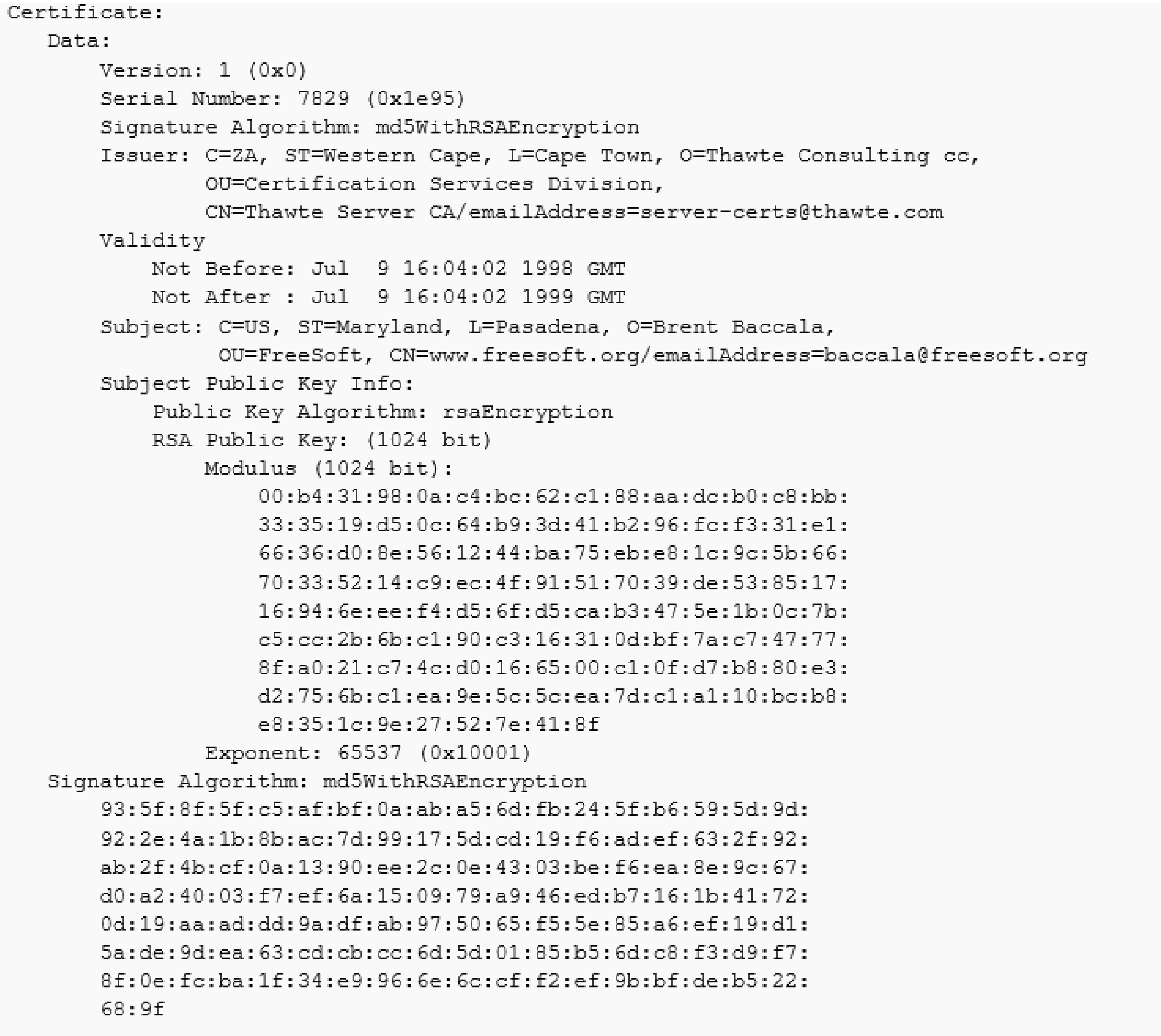
a) What is the validity of the certificate?

b) Is there any information related to RSA public key? If yes, what is the key?

c) Is there any information related to CRL (Certificate Revocation List)? If not, where should it be located?

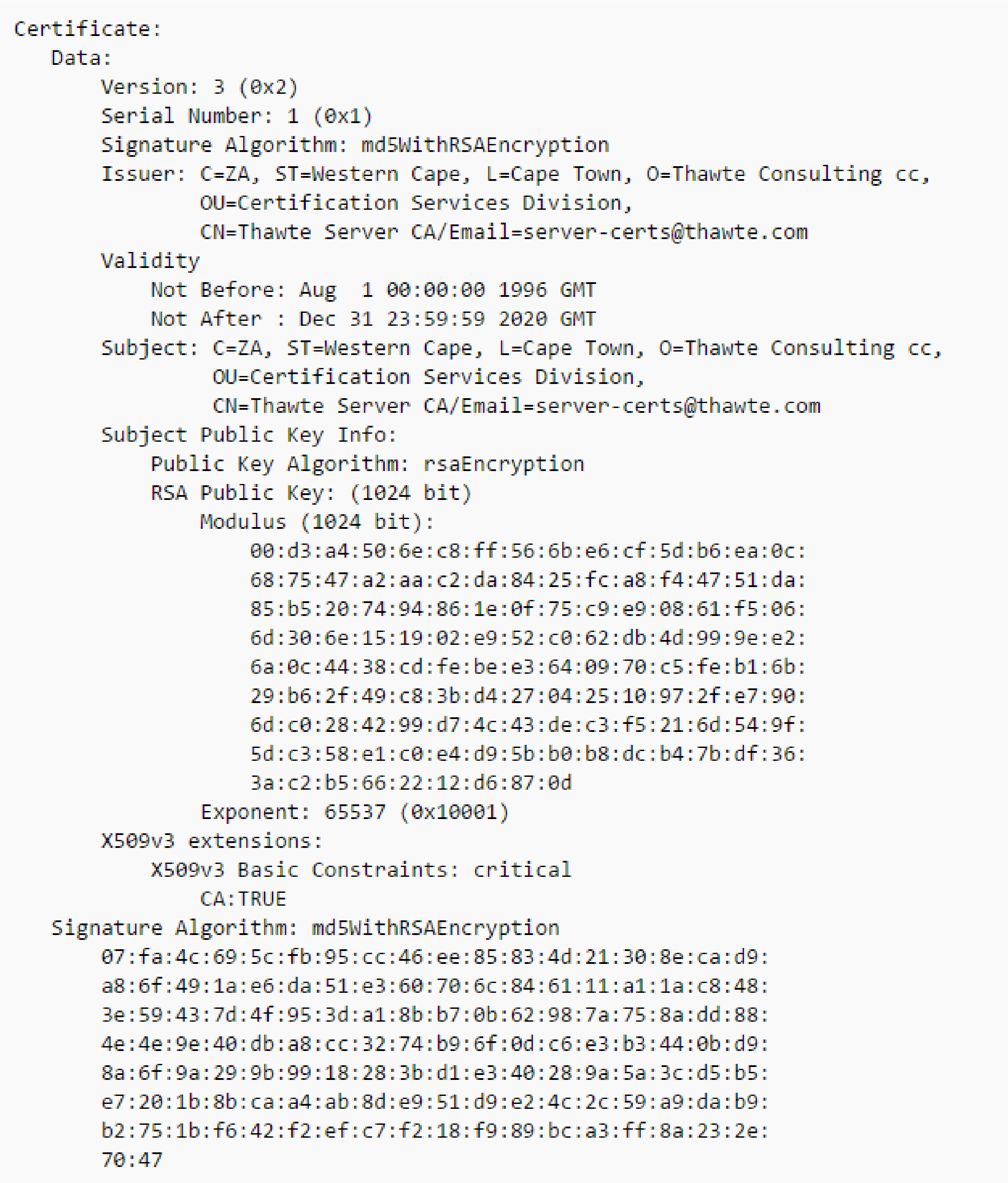
d) Notice that the ‘Issuer’ and the ‘Subject’ are the same organization. What does it mean?

CERTIFICATE 1



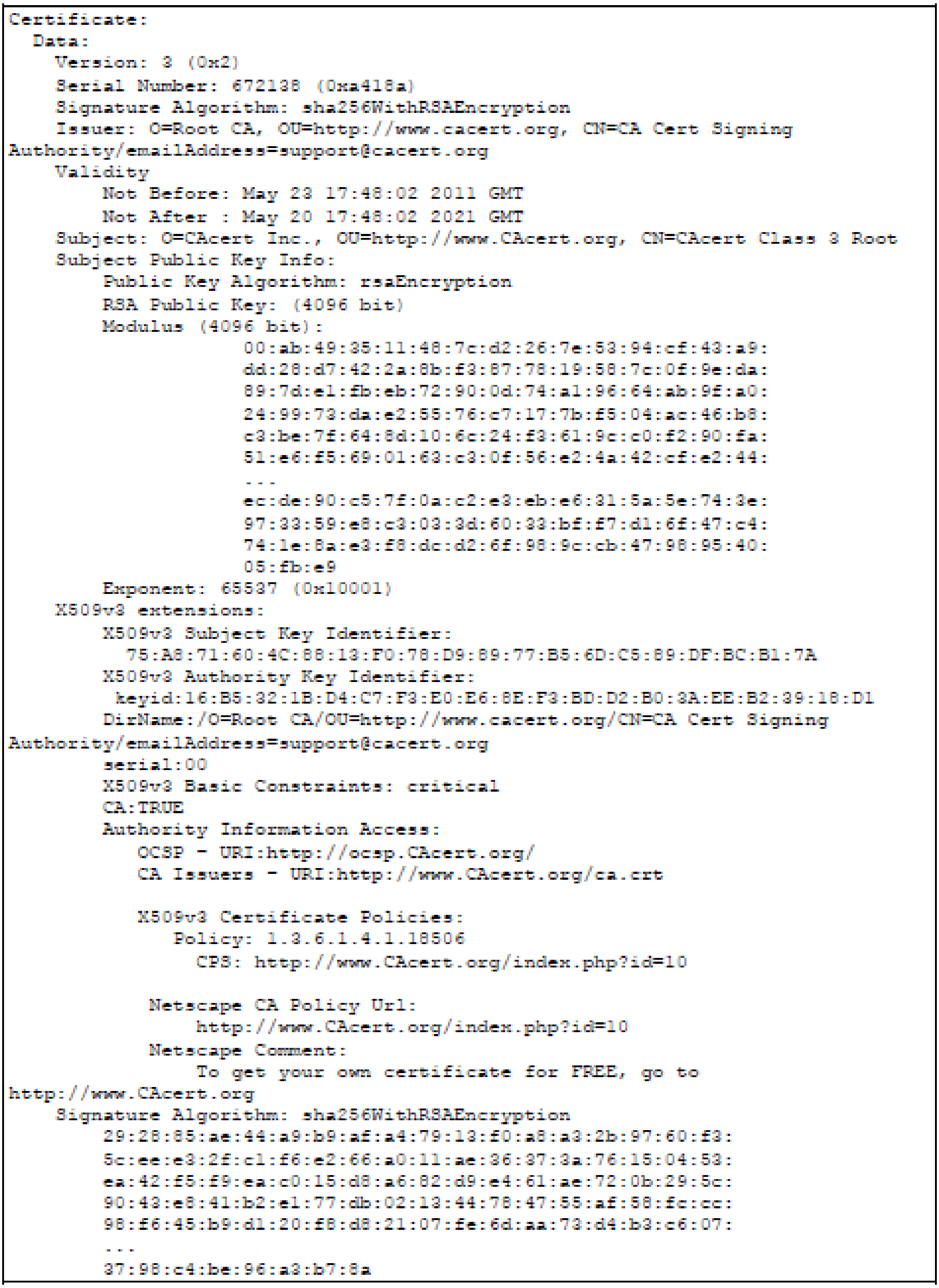
```
Certificate:
   Data:
       Version: 1 (0x0)
       Serial Number: 7829 (0x1e95)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Validity
           Not Before: Jul  9 16:04:02 1998 GMT
           Not After : Jul  9 16:04:02 1999 GMT
       Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
                OU=FreeSoft, CN=www.freesoft.org/emailAddress=baccala@freesoft.org
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
                   33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
                   66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
                   70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
                   16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
                   c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
                   8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
                   d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
                   e8:35:1c:9e:27:52:7e:41:8f
               Exponent: 65537 (0x10001)
   Signature Algorithm: md5WithRSAEncryption
       93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
       92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
       ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
       d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
       0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
       5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
       8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:
       68:9f
```

CERTIFICATE 2



```
Certificate:
   Data:
       Version: 3 (0x2)
       Serial Number: 1 (0x1)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/Email=server-certs@thawte.com
       Validity
           Not Before: Aug  1 00:00:00 1996 GMT
           Not After : Dec 31 23:59:59 2020 GMT
       Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/Email=server-certs@thawte.com
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
                   68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
                   85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
                   6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
                   6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
                   29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
                   6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
                   5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
                   3a:c2:b5:66:22:12:d6:87:0d
               Exponent: 65537 (0x10001)
       X509v3 extensions:
           X509v3 Basic Constraints: critical
               CA:TRUE
   Signature Algorithm: md5WithRSAEncryption
       07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
       a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
       3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
       4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
       8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
       e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
       b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
       70:47
```

CERTIFICATE 3

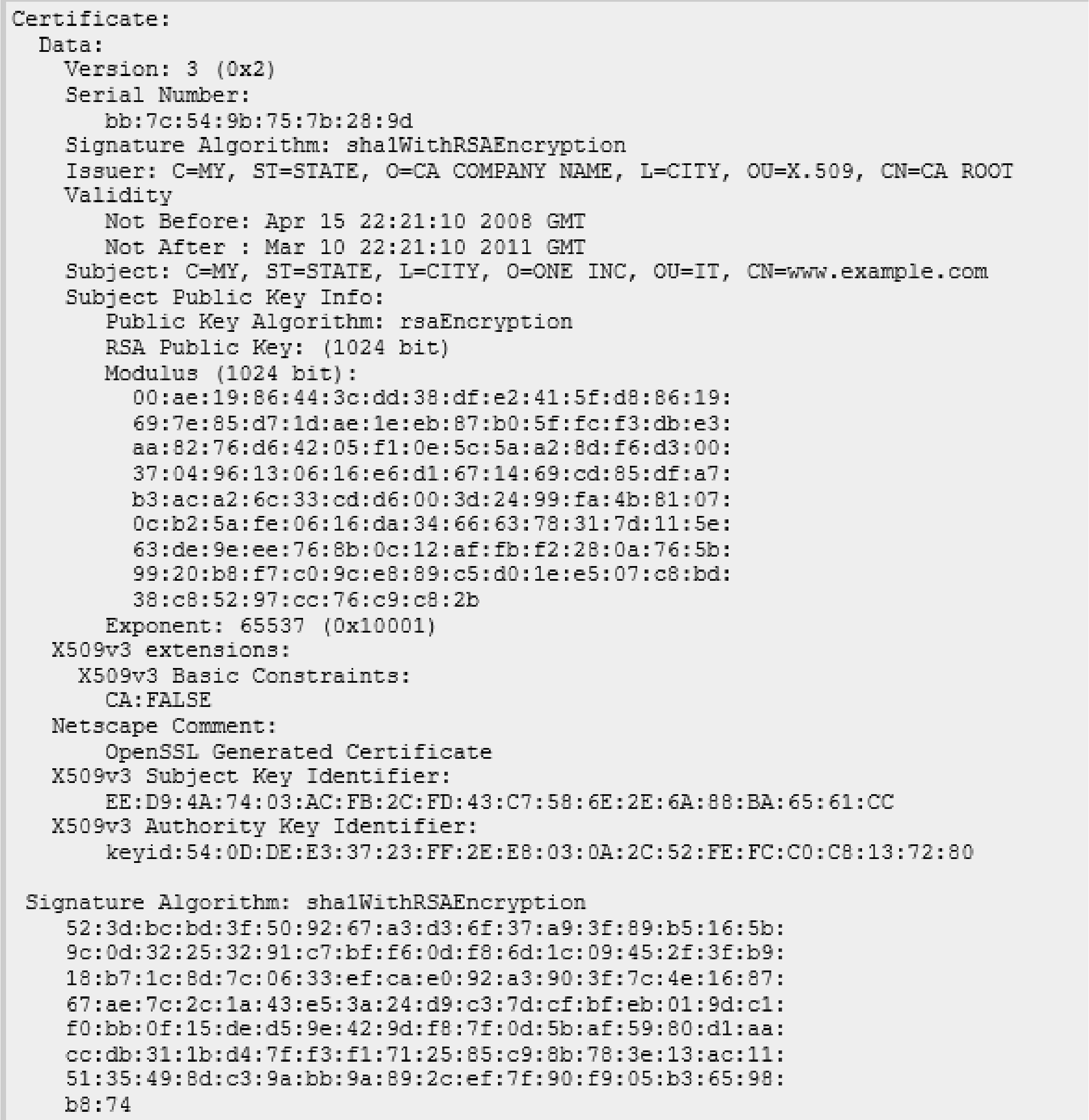


```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 672138 (0xa418a)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: O=Root CA, OU=http://www.cacert.org, CN=CA Cert Signing
Authority/emailAddress=support@cacert.org
    Validity
        Not Before: May 23 17:48:02 2011 GMT
        Not After : May 20 17:48:02 2021 GMT
    Subject: O=CAcert Inc., OU=http://www.CAcert.org, CN=CAcert Class 3 Root
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (4096 bit)
        Modulus (4096 bit):
                    00:ab:49:35:11:48:7c:d2:26:7e:53:94:cf:43:a9:
                    dd:28:d7:42:2a:8b:f3:87:78:19:58:7c:0f:9e:da:
                    89:7d:e1:fb:eb:72:90:0d:74:a1:96:64:ab:9f:a0:
                    24:99:73:da:e2:55:76:c7:17:7b:f5:04:ac:46:b8:
                    c3:be:7f:64:8d:10:6c:24:f3:61:9c:c0:f2:90:fa:
                    51:e6:f5:69:01:63:c3:0f:56:e2:4a:42:cf:e2:44:
                    ...
                    ec:de:90:c5:7f:0a:c2:e3:eb:e6:31:5a:5e:74:3e:
                    97:33:59:e8:c3:03:3d:60:33:bf:f7:d1:6f:47:c4:
                    74:1e:8a:e3:f8:dc:d2:6f:98:9c:cb:47:98:95:40:
                    05:fb:e9
        Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Key Identifier:
          75:A8:71:60:4C:88:13:F0:78:D9:89:77:B5:6D:C5:89:DF:BC:B1:7A
        X509v3 Authority Key Identifier:
         keyid:16:B5:32:1B:D4:C7:F3:E0:E6:8E:F3:BD:D2:B0:3A:EE:B2:39:18:D1
        DirName:/O=Root CA/OU=http://www.cacert.org/CN=CA Cert Signing
Authority/emailAddress=support@cacert.org
        serial:00
        X509v3 Basic Constraints: critical
        CA:TRUE
        Authority Information Access:
           OCSP - URI:http://ocsp.CAcert.org/
           CA Issuers - URI:http://www.CAcert.org/ca.crt

           X509v3 Certificate Policies:
              Policy: 1.3.6.1.4.1.18506
                CPS: http://www.CAcert.org/index.php?id=10

            Netscape CA Policy Url:
                http://www.CAcert.org/index.php?id=10
            Netscape Comment:
                To get your own certificate for FREE, go to
http://www.CAcert.org
    Signature Algorithm: sha256WithRSAEncryption
        29:28:85:ae:44:a9:b9:af:a4:79:13:f0:a8:a3:2b:97:60:f3:
        5c:ee:e3:2f:c1:f6:e2:66:a0:11:ae:36:37:3a:76:15:04:53:
        ea:42:f5:f9:ea:c0:15:d8:a6:82:d9:e4:61:ae:72:0b:29:5c:
        90:43:e8:41:b2:e1:77:db:02:13:44:78:47:55:af:58:fc:cc:
        98:f6:45:b9:d1:20:f8:d8:21:07:fe:6d:aa:73:d4:b3:c6:07:
        ...
        37:98:c4:be:96:a3:b7:8a
```

CERTIFICATE 4



```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
       bb:7c:54:9b:75:7b:28:9d
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=MY, ST=STATE, O=CA COMPANY NAME, L=CITY, OU=X.509, CN=CA ROOT
    Validity
       Not Before: Apr 15 22:21:10 2008 GMT
       Not After : Mar 10 22:21:10 2011 GMT
    Subject: C=MY, ST=STATE, L=CITY, O=ONE INC, OU=IT, CN=www.example.com
    Subject Public Key Info:
       Public Key Algorithm: rsaEncryption
       RSA Public Key: (1024 bit)
       Modulus (1024 bit):
         00:ae:19:86:44:3c:dd:38:df:e2:41:5f:d8:86:19:
         69:7e:85:d7:1d:ae:1e:eb:87:b0:5f:fc:f3:db:e3:
         aa:82:76:d6:42:05:f1:0e:5c:5a:a2:8d:f6:d3:00:
         37:04:96:13:06:16:e6:d1:67:14:69:cd:85:df:a7:
         b3:ac:a2:6c:33:cd:d6:00:3d:24:99:fa:4b:81:07:
         0c:b2:5a:fe:06:16:da:34:66:63:78:31:7d:11:5e:
         63:de:9e:ee:76:8b:0c:12:af:fb:f2:28:0a:76:5b:
         99:20:b8:f7:c0:9c:e8:89:c5:d0:1e:e5:07:c8:bd:
         38:c8:52:97:cc:76:c9:c8:2b
       Exponent: 65537 (0x10001)
   X509v3 extensions:
     X509v3 Basic Constraints:
       CA:FALSE
   Netscape Comment:
       OpenSSL Generated Certificate
   X509v3 Subject Key Identifier:
       EE:D9:4A:74:03:AC:FB:2C:FD:43:C7:58:6E:2E:6A:88:BA:65:61:CC
   X509v3 Authority Key Identifier:
       keyid:54:0D:DE:E3:37:23:FF:2E:E8:03:0A:2C:52:FE:FC:C0:C8:13:72:80

 Signature Algorithm: sha1WithRSAEncryption
    52:3d:bc:bd:3f:50:92:67:a3:d3:6f:37:a9:3f:89:b5:16:5b:
    9c:0d:32:25:32:91:c7:bf:f6:0d:f8:6d:1c:09:45:2f:3f:b9:
    18:b7:1c:8d:7c:06:33:ef:ca:e0:92:a3:90:3f:7c:4e:16:87:
    67:ae:7c:2c:1a:43:e5:3a:24:d9:c3:7d:cf:bf:eb:01:9d:c1:
    f0:bb:0f:15:de:d5:9e:42:9d:f8:7f:0d:5b:af:59:80:d1:aa:
    cc:db:31:1b:d4:7f:f3:f1:71:25:85:c9:8b:78:3e:13:ac:11:
    51:35:49:8d:c3:9a:bb:9a:89:2c:ef:7f:90:f9:05:b3:65:98:
    b8:74
```