University Of Washington, CSE 590P – Computer Security - Homework 7

Tadayoshi Kohno, John Manferdelli

Due: 4:30pm March 1, 2007.

See the course website (http://www.cs.washington.edu/education/courses/csep590b/07wi/) for instructions on how to submit your homework via the UW Catalyst Tools. For this assignment, you should submit a PDF file named 'YourLastName-YourFirstInitial-HW7.pdf. Please write your name on the first page. The entire assignment is worth 18 points and there is an opportunity for extra credit.

1. Certificate Evaluation [4]. Consider the certificates in appendix 1.
    a. For the first certificate, how long is this certificate valid? What is the purpose of the certificate?
    b. Reconstruct the certificate chain from the four certs, chaining on DN and SN and verifying validity rules
    c. Assume there is a UI that grants you express authority to examine the cert and accept it or not, what would you want to see in the UI? If you are running a "top secret" project where disclosure of information is critical to a project, what would your policy for installing certificates in the "trusted store" be?
2. Revocation [4]

    It has been observed that in normal commercial operation about 3% of previously valid certificates are revoked annually before expiry. The information required to record the revocation is about 32 bytes/revoked certificate.
    a. Verisign has about 500,000 active "high assurance" certs. What is the size of their CRL?
    b. Suppose that instead of CRL's, you implementation of revocation used OCSP, what are the bandwidth and "freshness" requirements for revocation? (You will need to make assumptions about how many times you use certs and how "fresh" your safety requirements are, please justify them).
    c. Consider a passport that comes with a certificate of identity and validity. There are about 60 million active passports in the US. What would you do for revocation?
3. DRM Attack model [10]
    a. Carefully explain the protection model for DRM based on the TPM and conformant hardware explained in class, observing the cryptographic assumptions, revocation and "liveness," distribution and assumptions on the software characteristics of the "DRM'd" applications, OS and hypervisor. Assume the hardware is "perfect" and that we are not concerned with hardware attacks.
    b. Discuss the "risk" and "threat" model for "big" DRM and "small" DRM and compare how the HW based model compares with traditional protection schemes on both PC's and cell phones. Be sure to consider the overall "management" of the system and its effect on customer satisfaction
    c. Now remove the "trusted HW" (i.e.-assume the DRM system has to run on existing PCs). What are the vulnerabilities, attacks, risk model assumptions.

Appendix 1 – Certs for Problem 1

Certificate 1

```
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number:
         61:02:28:4f:00:0a:00:01:6f:26
      Signature Algorithm: sha1WithRSAEncryption
      Issuer: CN=Microsoft Personnel E-Mail CA 1
      Validity
         Not Before: Sep 28 19:15:59 2006 GMT
         Not After : Sep 28 19:15:59 2007 GMT
      Subject: CN=John Manferdelli/emailAddress=jmanfer@microsoft.com
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
         RSA Public Key: (1024 bit)
            Modulus (1024 bit):
               00:ca:ee:c7:b4:e3:cf:80:d3:70:17:0b:1d:7f:d9:
               25:13:86:08:fd:8b:85:31:00:ab:20:2d:6d:31:9b:
               01:78:1e:8b:53:40:0b:3a:ed:77:de:16:5b:92:dc:
               35:a8:81:ce:5c:18:bb:79:97:ad:59:9c:76:c0:2a:
               e5:c0:e6:fe:79:49:37:da:bc:3d:03:43:a9:54:d2:
               14:5d:da:9b:02:39:d0:95:a7:91:0f:c3:55:bb:44:
               4c:bf:92:72:10:28:f8:4f:53:8c:71:27:b9:12:96:
               d8:17:a7:ce:90:a9:3b:87:4e:b8:45:52:a7:07:fe:
               fd:6d:4c:0b:a0:2b:20:3d:39
            Exponent: 65537 (0x10001)
      X509v3 extensions:
         X509v3 Key Usage:
            Digital Signature
         X509v3 Subject Key Identifier:
            C2:8C:7C:4E:B1:1C:15:25:F7:C1:E1:86:DE:13:27:AD:1C:EE:8A:0E
         1.3.6.1.4.1.311.21.7:
            0..&+.....7.....M.........}...t.O... ......e...
         X509v3 Authority Key Identifier:
            keyid:25:26:1D:87:CC:4B:55:0E:C0:93:0F:DB:1A:4B:DE:82:BE:A0:0E:E8

         X509v3 CRL Distribution Points:
            URI:http://crl.microsoft.com/pki/mscorp/crl/Microsoft%20Personnel%20E-
Mail%20CA%201(10).crl
            URI:http://corppki/crl/Microsoft%20Personnel%20E-Mail%20CA%201(10).crl

         Authority Information Access:
            CA Issuers - URI:http://corppki/aia/Microsoft%20Personnel%20E-Mail%20CA%201(10).crt
            CA Issuers - URI:http://www.microsoft.com/pki/mscorp/Microsoft%20Personnel%20E-
Mail%20CA%201(10).crt

         X509v3 Extended Key Usage:
            E-mail Protection
         1.3.6.1.4.1.311.21.10:
```

0.0
..+.....
X509v3 Subject Alternative Name:
email:jmanfer@microsoft.com
Signature Algorithm: sha1WithRSAEncryption
96:fe:f5:a9:ed:20:4f:c7:fe:ec:b8:47:31:43:5d:e4:9e:07:
66:bf:9c:df:34:e0:d5:2d:3d:57:f0:58:a8:92:cb:62:19:11:
15:99:fa:b0:41:24:e2:e9:13:92:94:19:9f:dc:f4:a9:13:76:
f0:46:c2:95:9f:0b:11:5e:8f:46:2f:9a:36:ef:15:3a:4c:c4:
8b:24:42:d9:e4:40:0a:e7:03:68:4b:fd:e6:9b:e1:bb:33:ce:
65:fa:ca:68:d2:f4:3d:3d:63:a9:f6:cd:a4:90:ef:23:84:2a:
5e:2d:d2:84:a8:37:7b:fe:0b:c8:b9:5e:66:75:cf:25:88:a7:
fd:f3:cf:16:ee:fa:ca:ea:b4:d7:92:1c:7a:03:b9:19:e1:2a:
67:00:c4:4c:48:90:0f:19:51:09:33:c2:0a:c4:d1:6e:fc:53:
14:2c:58:9c:e8:56:a3:2c:b6:78:08:0d:2c:b9:9c:3d:33:9a:
80:f9:2d:77:a0:c7:5c:17:ba:54:33:05:c6:15:41:b2:cc:1f:
5c:85:d4:34:ce:ab:28:19:c2:6a:43:e8:d2:30:28:b4:ad:b3:
f0:5e:e1:71:8a:0f:aa:06:59:87:7c:db:14:07:23:21:7e:6f:
c8:bd:40:c9:4b:d6:16:c9:7a:2d:74:32:d6:32:76:52:eb:32:
8d:55:fb:01
-----BEGIN CERTIFICATE-----
MIIEyTCCA7GgAwIBAgIKYQIoTwAKAAFvJjANBgkqhkiG9w0BAQUFADAqMSgwJgYD
VQQDEx9NaWNyb3NvZnQgUGVyc29ubmVsIEUtTWFpbCBDQSAxMB4XDTA2MDkyODE5
MTU1OVoXDTA3MDkyODE5MTU1OVowQTEZMBcGA1UEAxMQSm9obiBNYW5mZXJkZWxs
aTEkMCIGCSqGSIb3DQEJARYVam1hbmZlckBtaWNyb3NvZnQuY29tMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQDK7se048+A03AXCx1/2SUThgj9i4UxAKsgLW0x
mwF4HotTQAs67XfeFluS3DWogc5cGLt5l61ZnHbAKuXA5v55STfavD0DQ6lU0hRd
2psCOdCVp5EPw1W7REy/knIQKPhPU4xxJ7kSltgXp86QqTuHTrhFUqcH/v1tTAug
KyA9OQIDAQABo4ICXDCCAlgwCwYDVR0PBAQDAgeAMB0GA1UdDgQWBBTCjHxOsRwV
JffB4YbeEyetHO6KDjA9BgkrBgEEAYI3FQcEMDAuBiYrBgEEAYI3FQiDz4lNrfIC
haGfDIL6yn2B4ft0gU+FqvYggei6CAIBZQIBADAfBgNVHSMEGDAWgBQlJh2HzEtV
DsCTD9saS96CvqAO6DCBsQYDVR0fBIGpMIGmMIGjoIGgoIGdhldodHRwOi8vY3Js
Lm1pY3Jvc29mdC5jb20vcGtpL21zY29ycC9jcmwvTWljcm9zb2Z0JTIwUGVyc29u
bmVsJTIwRS1NYWlsJTIwQ0ElMjAxKDEwKS5jcmyGQmh0dHA6Ly9jb3JwcGtpL2Ny
bC9NaWNyb3NvZnQlMjBQZXJzb25uZWwlMjBFLU1haWwlMjBDQSUyMDEoMTApLmNy
bDCBwQYIKwYBBQUHAQEEgbQwgbEwTgYIKwYBBQUHMAKGQmh0dHA6Ly9jb3JwcGtp
L2FpYS9NaWNyb3NvZnQlMjBQZXJzb25uZWwlMjBFLU1haWwlMjBDQSUyMDEoMTAp
LmNydDBfBggrBgEFBQcwAoZTaHR0cDovL3d3dy5taWNyb3NvZnQuY29tL3BraS9t
c2NvcnAvTWljcm9zb2Z0JTIwUGVyc29ubmVsJTIwRS1NYWlsJTIwQ0ElMjAxKDEw
KS5jcnQwEwYDVR0lBAwwCgYIKwYBBQUHAwQwGwYJKwYBBAGCNxUKBA4wDDAKBggr
BgEFBQcDBDAgBgNVHREEGTAXgRVqbWFuZmVyQG1pY3Jvc29mdC5jb20wDQYJKoZI
hvcNAQEFBQADggEBAJb+9antIE/H/uy4RzFDXeSeB2a/nN804NUtPVfwWKiSy2IZ
ERWZ+rBBJOLpE5KUGZ/c9KkTdvBGwpWfCxFej0YvmjbvFTpMxIskQtnkQArnA2hL
/eab4bszzmX6ymjS9D09Y6n2zaSQ7yOEKl4t0oSoN3v+C8i5XmZ1zyWIp/3zzxbu
+srqtNeSHHoDuRnhKmcAxExlkA8ZUQkzwgrE0W78UxQsWJzoVqMstnglDSy5nD0z
moD5LXegx1wXulQzBcYVQbLMH1yF1DTOqygZwmpD6NIwKLSts/Be4XGKD6oGWYd8
2xQHIyF+b8i9QMlL1hbJei10MtYydlLrMo1V+wE=
-----END CERTIFICATE-----

<u>Certificate 2</u>

Certificate:
Data:

Version: 1 (0x0)
Serial Number: 421 (0x1a5)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=US, O=GTE Corporation, OU=GTE CyberTrust Solutions, Inc., CN=GTE CyberTrust Global Root
Validity
Not Before: Aug 13 00:29:00 1998 GMT
Not After : Aug 13 23:59:00 2018 GMT
Subject: C=US, O=GTE Corporation, OU=GTE CyberTrust Solutions, Inc., CN=GTE CyberTrust Global Root
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:95:0f:a0:b6:f0:50:9c:e8:7a:c7:88:cd:dd:17:
0e:2e:b0:94:d0:1b:3d:0e:f6:94:c0:8a:94:c7:06:
c8:90:97:c8:b8:64:1a:7a:7e:6c:3c:53:e1:37:28:
73:60:7f:b2:97:53:07:9f:53:f9:6d:58:94:d2:af:
8d:6d:88:67:80:e6:ed:b2:95:cf:72:31:ca:a5:1c:
72:ba:5c:02:e7:64:42:e7:f9:a9:2c:d6:3a:0d:ac:
8d:42:aa:24:01:39:e6:9c:3f:01:85:57:0d:58:87:
45:f8:d3:85:aa:93:69:26:85:70:48:80:3f:12:15:
c7:79:b4:1f:05:2f:3b:62:99
Exponent: 65537 (0x10001)
Signature Algorithm: md5WithRSAEncryption
6d:eb:1b:09:e9:5e:d9:51:db:67:22:61:a4:2a:3c:48:77:e3:
a0:7c:a6:de:73:a2:14:03:85:3d:fb:ab:0e:30:c5:83:16:33:
81:13:08:9e:7b:34:4e:df:40:c8:74:d7:b9:7d:dc:f4:76:55:
7d:9b:63:54:18:e9:f0:ea:f3:5c:b1:d9:8b:42:1e:b9:c0:95:
4e:ba:fa:d5:e2:7c:f5:68:61:bf:8e:ec:05:97:5f:5b:b0:d7:
a3:85:34:c4:24:a7:0d:0f:95:93:ef:cb:94:d8:9e:1f:9d:5c:
85:6d:c7:aa:ae:4f:1f:22:b5:cd:95:ad:ba:a7:cc:f9:ab:0b:
7a:7f
-----BEGIN CERTIFICATE-----
MIICWjCCAcMCAgGlMA0GCSqGSIb3DQEBBAUAMHUxCzAJBgNVBAYTAlVTMRgwFgYD
VQQKEw9HVEUgQ29ycG9yYXRpb24xJzAlBgNVBAsTHkdURSBDeWJlclRydXN0IFNv
bHV0aW9ucywgSW5jLjEjMCEGA1UEAxMaR1RFIEN5YmVyVHJ1c3QgR2xvYmFsIFJv
b3QwHhcNOTgwODEzMDAyOTAwWhcNMTgwODEzMjM1OTAwWjB1MQswCQYDVQQGEwJV
UzEYMBYGA1UEChMPR1RFIENvcnBvcmF0aW9uMScwJQYDVQQLEx5HVEUgQ3liZXJU
cnVzdCBTb2x1dGlvbnMsIEluYy4xIzAhBgNVBAMTGkdURSBDeWJlclRydXN0IEds
b2JhbCBSb290MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCVD6C28FCc6HrH
iM3dFw4usJTQGz0O9pTAipTHBsiQl8i4ZBp6fmw8U+E3KHNgf7KXUwefU/ltWJTS
r41tiGeA5u2ylc9yMcqlHHK6XALnZELn+aks1joNrI1CqiQBOeacPwGFVw1Yh0X4
04Wqk2kmhXBIgD8SFcd5tB8FLztimQIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAG3r
GwnpXtlR22ciYaQqPEh346B8pt5zohQDhT37qw4wxYMWM4ETCJ57NE7fQMh017l9
3PR2VX2bY1QY6fDq81yx2YtCHrnAlU66+tXifPVoYb+O7AWXX1uw16OFNMQkpw0P
lZPvy5TYnh+dXIVtx6quTx8itc2VrbqnzPmrC3p/
-----END CERTIFICATE-----

<u>Certificate 3</u>

Certificate:
Data:
Version: 3 (0x2)

```
        Serial Number:
            61:2a:50:23:00:03:00:00:00:13
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=Microsoft Internet Authority
        Validity
            Not Before: Apr 21 19:10:19 2006 GMT
            Not After : Apr 19 23:59:00 2009 GMT
        Subject: CN=Microsoft Personnel E-Mail CA 1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:cc:8a:de:41:0e:4a:63:8a:23:43:a3:43:49:99:
                    61:33:04:24:c0:76:9f:f7:47:77:99:9c:64:b1:4e:
                    56:dd:d7:1a:75:b8:c8:d6:c9:6c:93:df:ed:f6:ab:
                    44:92:15:75:db:a0:1a:0c:16:dc:f7:64:f2:5a:c5:
                    8f:58:0b:fd:ff:fd:74:87:47:e0:a7:15:7b:ba:3b:
                    c1:d6:b8:63:ed:50:4d:1e:b7:c2:24:94:d1:86:58:
                    3c:40:79:9d:34:6a:2d:a0:21:4d:0b:58:44:f5:ed:
                    d3:da:b7:f9:aa:2f:c9:e4:a2:3f:38:30:16:53:58:
                    b7:19:4e:c2:5b:dd:e0:a4:7e:28:16:85:f1:47:af:
                    51:ff:1c:db:36:0b:2f:d8:7e:4f:12:9b:65:2d:f1:
                    fa:e7:87:ae:93:ff:db:8d:72:72:d8:98:d7:22:09:
                    1f:9d:28:a0:08:21:61:0d:10:cb:f6:9e:ab:8e:71:
                    62:55:ef:c8:84:d3:c6:09:62:14:96:be:1c:9a:3e:
                    28:11:65:8c:d1:3a:51:75:82:53:52:77:71:8f:e8:
                    38:61:84:53:e0:7b:cb:c0:52:7e:74:29:a6:e2:08:
                    09:43:99:cf:72:e0:fd:b1:5c:14:64:a2:a3:62:b5:
                    ac:da:57:84:91:51:5c:0e:75:b9:3e:e2:04:d8:3c:
                    c8:df
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:1
            X509v3 Subject Key Identifier:
                25:26:1D:87:CC:4B:55:0E:C0:93:0F:DB:1A:4B:DE:82:BE:A0:0E:E8
            X509v3 Key Usage:
                Digital Signature, Certificate Sign, CRL Sign
            1.3.6.1.4.1.311.21.1:
                ..
.

            1.3.6.1.4.1.311.21.2:
                ......f.d.E....f.N%..-
            1.3.6.1.4.1.311.20.2:
                .
.S.u.b.C.A
            X509v3 Authority Key Identifier:
                keyid:33:5F:DD:0F:B7:9C:5C:CE:EE:87:DD:70:70:8B:5F:7D:CF:22:BC:B9

            X509v3 CRL Distribution Points:
                URI:http://crl.microsoft.com/pki/mscorp/crl/mswww(3).crl
                URI:http://corppki/crl/mswww(3).crl
```

Authority Information Access:
CA Issuers - URI:http://www.microsoft.com/pki/mscorp/mswww(3).crt
CA Issuers - URI:http://corppki/aia/mswww(3).crt

Signature Algorithm: sha1WithRSAEncryption
67:91:97:d1:06:b7:42:3f:ab:27:fb:ed:02:51:40:05:48:c9:
f2:31:38:7e:b2:63:a8:eb:3e:f5:ef:a5:8d:45:ca:4b:15:cf:
4e:54:69:c3:6d:f0:e5:0f:6c:60:64:e6:6b:63:ef:44:83:dc:
bc:d3:a3:d2:c2:0e:dc:1a:ca:85:31:bc:c3:fc:2f:ce:9d:ff:
b4:7f:c7:b1:74:b4:3d:59:14:2b:d2:eb:49:1a:4d:f6:6e:db:
fe:65:3b:21:5e:fc:10:f3:01:f6:de:d3:90:97:d0:f4:04:9a:
c6:5c:2c:f7:89:3b:d0:df:3c:81:ad:e1:d2:e5:5c:5c:44:75:
5e:98:7a:45:8e:67:db:20:05:f4:70:f7:06:57:01:7d:60:a9:
16:71:f2:0c:40:94:20:3c:82:f5:8f:2f:7b:86:10:74:28:19:
64:c7:e9:7e:c8:3a:ad:1c:5b:53:c4:40:b6:d8:fa:9f:8b:f5:
43:a8:61:cf:98:9d:0a:11:6d:b7:6e:e7:13:e8:ff:78:9b:6a:
e8:bc:7c:92:4c:de:38:4e:9c:ab:48:8a:f6:5b:c1:99:cf:fe:
69:65:21:18:c2:e1:3a:01:3d:d0:ab:74:f5:81:8b:c5:65:b3:
4b:5d:99:42:bc:2e:2c:5f:18:92:b6:48:69:4f:71:d2:c7:59:
95:8c:3b:36
-----BEGIN CERTIFICATE-----
MIIEczCCA1ugAwIBAgIKYSpQIwADAAAAEzANBgkqhkiG9w0BAQUFADAnMSUwIwYD
VQQDExxNaWNyb3NvZnQgSW50ZXJuZXQgQXV0aG9yaXR5MB4XDTA2MDQyMTE5MTAx
OVoXDTA5MDQxOTIzNTkwMFowKjEoMCYGA1UEAxMfTWljcm9zb2Z0IFBlcnNvbm5l
bCBFLU1haWwgQ0EgMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMyK
3kEOSmOKI0OjQ0mZYTMEJMB2n/dHd5mcZLFOVt3XGnW4yNbJbJPf7farRJIVddug
GgwW3Pdk8lrFj1gL/f/9dIdH4KcVe7o7wda4Y+1QTR63wiSU0YZYPEB5nTRqLaAh
TQtYRPXt09q3+aovyeSiPzgwFlNYtxlOwlvd4KR+KBaF8UevUf8c2zYLL9h+TxKb
ZS3x+ueHrpP/241yctiY1yIJH50ooAghYQ0Qy/aeq45xYlXvyITTxgliFJa+HJo+
KBFljNE6UXWCU1J3cY/oOGGEU+B7y8BSfnQppuIICUOZz3Lg/bFcFGSio2K1rNpX
hJFRXA51uT7iBNg8yN8CAwEAAaOCAZwwggGYMBIGA1UdEwEB/wQIMAYBAf8CAQEw
HQYDVR0OBBYEFCUmHYfMS1UOwJMP2xpL3oK+oA7oMAsGA1UdDwQEAwIBhjASBgkr
BgEEAYI3FQEEBQIDCgAKMCMGCSsGAQQBgjcVAgQWBBSkrJYTZhRkAUXmvAzaZplO
JagELTAZBgkrBgEEAYI3FAIEDB4KAFMAdQBiAEMAQTAfBgNVHSMEGDAWgBQzX90P
t5xczu6H3XBwi199zyK8uTBmBgNVHR8EXzBdMFugWaBXhjRodHRwOi8vY3JsLm1p
Y3Jvc29mdC5jb20vcGtpL21zY29ycC9jcmwvbXN3d3coMykuY3Jshh9odHRwOi8v
Y29ycHBraS9jcmwvbXN3d3coMykuY3JsMHkGCCsGAQUFBwEBBG0wazA8BggrBgEF
BQcwAoYwaHR0cDovL3d3dy5taWNyb3NvZnQuY29tL3BraS9tc2NvcnAvbXN3d3co
MykuY3J0MCsGCCsGAQUFBzAChh9odHRwOi8vY29ycHBraS9haWEvbXN3d3coMyku
Y3J0MA0GCSqGSIb3DQEBBQUAA4IBAQBnkZfRBrdCP6sn++0CUUAFSMnyMTh+smOo
6z7176WNRcpLFc9OVGnDbfDlD2xgZOZrY+9Eg9y806PSwg7cGsqFMbzD/C/Onf+0
f8exdLQ9WRQr0utJGk32btv+ZTshXvwQ8wH23tOQl9D0BJrGXCz3iTvQ3zyBreHS
5VxcRHVemHpFjmfbIAX0cPcGVwF9YKkWcfIMQJQgPIL1jy97hhB0KBlkx+l+yDqt
HFtTxEC22Pqfi/VDqGHPmJ0KEW23bucT6P94m2rovHySTN44TpyrSIr2W8GZz/5p
ZSEYwuE6AT3Qq3T1gYvFZbNLXZlCvC4sXxiStkhpT3HSx1mVjDs2
-----END CERTIFICATE-----

Certificate 4

Certificate:
Data:

```
        Version: 3 (0x2)
        Serial Number: 67109886 (0x40003fe)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=GTE Corporation, OU=GTE CyberTrust Solutions, Inc., CN=GTE CyberTrust Global Root
        Validity
          Not Before: Apr 19 14:35:00 2006 GMT
          Not After : Apr 19 23:59:00 2009 GMT
        Subject: CN=Microsoft Internet Authority
        Subject Public Key Info:
          Public Key Algorithm: rsaEncryption
          RSA Public Key: (2048 bit)
            Modulus (2048 bit):
              00:b5:08:6e:4d:18:76:c4:d7:9c:63:ec:c2:ac:7c:
              77:f3:6d:ae:c8:f2:f1:66:ae:f1:c2:87:04:60:6e:
              29:9c:00:65:ee:6a:5b:e4:0e:53:88:11:c6:22:9b:
              33:fb:6b:b2:91:2e:d6:53:9b:53:be:cf:56:d8:99:
              4a:a1:50:32:45:ce:60:d2:e1:96:ad:5a:fd:ea:a1:
              eb:c4:49:27:1c:5e:bf:d2:96:99:fa:69:43:7f:3c:
              38:da:a1:8b:cc:33:88:7a:17:73:ae:91:50:28:aa:
              69:ba:7b:e7:57:5b:9b:09:e7:4c:de:86:7c:84:7d:
              e7:66:60:f9:a6:f5:c2:61:8b:de:8e:c1:d5:e7:c2:
              30:22:3d:2c:83:0a:b0:87:75:eb:21:e2:5c:a6:d3:
              04:7b:96:9e:40:1e:e1:0c:76:04:c0:20:a0:94:10:
              db:51:1b:4c:18:72:bc:27:dd:12:24:5d:39:d6:28:
              d4:e4:de:db:18:a1:e0:95:0f:99:77:fb:c4:f3:43:
              8c:c0:ab:a6:31:09:f3:0a:31:80:29:c7:d7:6c:fb:
              3c:d3:ea:c2:b8:67:15:ef:fa:f3:4f:2d:6b:1c:b8:
              88:d8:0e:6d:77:19:4b:71:11:71:90:40:f5:11:53:
              d7:3d:e8:9d:0d:84:da:99:64:68:13:e6:65:03:e2:
              66:ed
            Exponent: 65537 (0x10001)
        X509v3 extensions:
          X509v3 CRL Distribution Points:
            URI:http://www.public-trust.com/cgi-bin/CRL/2018/cdp.crl

          X509v3 Subject Key Identifier:
            33:5F:DD:0F:B7:9C:5C:CE:EE:87:DD:70:70:8B:5F:7D:CF:22:BC:B9
          X509v3 Certificate Policies:
            Policy: 1.2.840.113763.1.2.1.5
              CPS: http://www.public-trust.com/CPS/OmniRoot.html

          X509v3 Authority Key Identifier:
            DirName:/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust
Global Root
            serial:01:A5

          X509v3 Key Usage: critical
            Digital Signature, Certificate Sign, CRL Sign
          X509v3 Basic Constraints: critical
            CA:TRUE, pathlen:2
    Signature Algorithm: sha1WithRSAEncryption
        63:49:09:54:ed:c5:db:9e:78:19:00:83:9a:e3:37:22:fb:56:
        76:5c:54:d3:c8:e1:5c:fd:37:dc:d2:a5:3f:c5:55:8f:64:f0:
```

49:77:1d:94:56:4d:b2:0b:09:88:1c:50:58:38:94:90:0b:ee:
ca:9f:b1:84:e6:71:37:ac:10:32:06:b9:c1:d2:8c:a6:05:c0:
5e:0f:cb:53:dc:1e:01:df:58:c7:7e:71:60:b0:2f:54:62:29:
fd:b8:93:75:e3:8f:9e:b5:bc:ce:7a:05:20:e2:a6:8d:02:90:
1a:58:6a:de:dd:86:3b:00:b9:f5:cb:fe:97:82:a2:04:20:46:
5c:09

-----BEGIN CERTIFICATE-----
MIIECzCCA3SgAwIBAgIEBAAD/jANBgkqhkiG9w0BAQUFADB1MQswCQYDVQQGEwJV
UzEYMBYGA1UEChMPR1RFIENvcnBvcmF0aW9uMScwJQYDVQQLEx5HVEUgQ3liZXJU
cnVzdCBTb2x1dGlvbnMsIEluYy4xIzAhBgNVBAMTGkdURSBDeWJlclRydXN0IEds
b2JhbCBSb290MB4XDTA2MDQxOTE0MzUwMFoXDTA5MDQxOTIzNTkwMFowJzElMCMG
A1UEAxMcTWljcm9zb2Z0IEludGVybmV0IEF1dGhvcml0eTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALUIbk0YdsTXnGPswqx8d/Ntrsjy8Wau8cKHBGBu
KZwAZe5qW+QOU4gRxiKbM/trspEu1lObU77PVtiZSqFQMkXOYNLhlq1a/eqh68RJ
Jxxev9KWmfppQ388ONqhi8wziHoXc66RUCiqabp751dbmwnnTN6GfIR952Zg+ab1
wmGL3o7B1efCMCI9LIMKsId16yHiXKbTBHuWnkAe4Qx2BMAgoJQQ21EbTBhyvCfd
EiRdOdYo1OTe2xih4JUPmXf7xPNDjMCrpjEJ8woxgCnH12z7PNPqwrhnFe/6808t
axy4iNgObXcZS3ERcZBA9RFT1z3onQ2E2plkaBPmZQPiZu0CAwEAAaOCAXAwggFs
MEUGA1UdHwQ+MDwwOqA4oDaGNGh0dHA6Ly93d3cucHVibGljLXRydXN0LmNvbS9j
Z2ktYmluL0NSTC8yMDE4L2NkcC5jcmwwHQYDVR0OBBYEFDNf3Q+3nFzO7ofdcHCL
X33PIry5MFQGA1UdIARNMEswSQYKKoZIhvhjAQIBBTA7MDkGCCsGAQUFBwIBFi1o
dHRwOi8vd3d3LnB1YmxpYy10cnVzdC5jb20vQ1BTL09tbmlSb290Lmh0bWwwgYkG
A1UdIwSBgTB/oXmkdzB1MQswCQYDVQQGEwJVUzEYMBYGA1UEChMPR1RFIENvcnBv
cmF0aW9uMScwJQYDVQQLEx5HVEUgQ3liZXJUcnVzdCBTb2x1dGlvbnMsIEluYy4x
IzAhBgNVBAMTGkdURSBDeWJlclRydXN0IEdsb2JhbCBSb290ggIBpTAOBgNVHQ8B
Af8EBAMCAYYwEgYDVR0TAQH/BAgwBgEB/wIBAjANBgkqhkiG9w0BAQUFAAOBgQBj
SQlU7cXbnngZAIOa4zci+1Z2XFTTyOFc/Tfc0qU/xVWPZPBJdx2UVk2yCwmIHFBY
OJSQC+7Kn7GE5nE3rBAyBrnB0oymBcBeD8tT3B4B31jHfnFgsC9UYin9uJN144+e
tbzOegUg4qaNApAaWGre3YY7ALn1y/6XgqIEIEZcCQ==
-----END CERTIFICATE-----