Cert Logik

Tools
About
Links

CSR and Certificate Decoder (Also Decodes PKCS#7 Certificate Chains)
CSR Decoder And Certificate Decoder
Try Our New Decoder Today

```
-----BEGIN CERTIFICATE-----
MIIIiTCCBnGgAwIBAgIQP1nUyf4TRwPZ+Ou88ceQqzANBgkqhkiG9w0BAQwFADBE
MQswCQYDVQQGEwJOTDEZMBcGA1UEChMQR0VBTlQgVmVyZW5pZ2luZzEaMBgGA1UE
AxMRR0VBTlQgT1YgUlNBIENBIDQwHhcNMjQwNDIyMDAwMDAwWhcNMjUwNDIyMjM1
OTU5WjCBiDELMAkGA1UEBhMCQkUxJzAlBgNVBAgMHkJydXhlbGxlcy1DYXBpdGFs
ZSwgUsOpZ2lvbiBkZTEoMCYGA1UEChMfU2Vydmljz2SBQdWJsaWMgRmVkZXJhbCBG
aW5hbmNlczEmMCQGA1UEAxMdZnBzZmluYW5jZXNzc2wubWluZmluLmZnb3YuYmUw
ggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDJqdS3voeHszaTqM65j8FF
WCjerMrLt/dZNX9eh/s7nVkCH/UmKm2uTUv5j/iJfP+Ku0dV6MJ2fmTYKIgC+XXj
83PpbqeQI4m8mTTyN2WHy8ysOVfbp9QBQfjQlADk9stSUugYH3QvcZ4o0aomK+cU
6XE5wFtEghlZ69pEEtYithv+T0+v9Qmjn6cx198YghbiKNAwYl9IauO12PP0aMPK
J8L8U5JLUIW4xAphST/xThQUsNl4KlDQHoRNkI9p1O5AFBzSBIAYviSEDUph/Rh/
qFyIXyrlHhyrmBwaKvGznEnG08G8PDNJ5IGWifBNbjLdS/DZW+e5sED1EJhoo9ur
ulpGnYxMdrM0qjsKuar5hiEmls2QW4q33pMpYlNIbLAlcOvL0nz0QazLzKz4jjNm
qiG4USpSPjidts8lshgNE0WmVHc1hgsV9UF2TWGoaP109uxwR6oWfvg05BVrOfrv
hK5rT5irRWRime5UsFEgxGLLuGCWKR2uhJkZLrjHd5RqNIuqgPVxmv/FXxWzv3BL
sRYHMwKmMUGvDSbAkZV0gwZ4wMLzTO1wbPYHNoGezUZQNUZkh3bN5xrphdn8cHgZ
01gbUm89A38kH5xDAvq3vzUGDxcCr9bNelnn8e2RU4inmA0uqiYzgrTChyFLsAvx
I/AlNBOVI5jB/NpsGlwxlwIDAQABo4IDMDCCAywwHwYDVR0jBBgwFoAUbx01SRBs
MvpZoJ68iugflb5xegwwHQYDVR0OBBYEFH6z+PA3ZwWarS6pJtIzFvucDBhLMA4G
A1UdDwEB/wQEAwIFoDAMBgNVHRMBAf8EAjAAMB0GA1UdJQQWMBQGCCsGAQUFBwMB
BggrBgEFBQcDAjBJBgNVHSAEQjBAMDQGCysGAQQBsjEBAgJPMCUwIwYIKwYBBQUH
AgEWF2h0dHBzOi8vc2VjdGlnby5jb20vQ1BTMAgGBmeBDAECAjA/BgNVHR8EODA2
```

Decode

Certificate Checks

Status	Check	Information
✓	Valid To	22 Apr 2025 (365 days)
✓	Weak-Key	Does not use a key on our blacklist - this is good
✓	Key-Size	4096 bits
✓	Signature Algorithm	Strong (sha384WithRSAEncryption)

Certificate Summary
Subject

RDN	Value
Common Name (CN)	fpsfinancesssl.minfin.fgov.be
Organization (O)	Service Public Federal Finances
State (ST)	Bruxelles-Capitale\, R\\xC3\\xA9gion de
Country (C)	BE

Properties

Property	Value
Issuer	CN = GEANT OV RSA CA 4,O = GEANT Vereniging,C = NL
Subject	CN = fpsfinancesssl.minfin.fgov.be,O = Service Public Federal Finances,ST = Bruxelles-Capitale\, R\C3\A9gion de,C = BE
Valid From	22 Apr 2024, midnight
Valid To	22 Apr 2025, 11:59 p.m.
Serial Number	3F:59:D4:C9:FE:13:47:03:D9:F8:EB:BC:F1:C7:90:AB (84207794029188436617402196364118954155)
CA Cert	No
Key Size	4096 bits

Property	Value
Fingerprint (SHA-1)	5C:0E:79:92:09:5E:95:1B:D7:3E:B5:BF:F3:FC:65:CB:B5:9D:CD:95
Fingerprint (MD5)	98:78:4E:82:63:B2:31:98:8B:E5:52:71:AC:8D:B7:C8
SANS	fpsfinancesssl.minfin.fgov.be

Certificate Detailed Information

```
Certificate:
Data:
    Version: 3 (0x2)
    Serial Number:
        3f:59:d4:c9:fe:13:47:03:d9:f8:eb:bc:f1:c7:90:ab
Signature Algorithm: sha384WithRSAEncryption
    Issuer:
        commonName                = GEANT OV RSA CA 4
        organizationName          = GEANT Vereniging
        countryName               = NL
    Validity
        Not Before: Apr 22 00:00:00 2024 GMT
        Not After : Apr 22 23:59:59 2025 GMT
    Subject:
        commonName                = fpsfinancesssl.minfin.fgov.be
        organizationName          = Service Public Federal Finances
        stateOrProvinceName       = Bruxelles-Capitale, R\E9gion de
        countryName               = BE
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (4096 bit)
            Modulus:
                00:c9:a9:d4:b7:be:87:87:b3:36:93:a8:ce:b9:8f:
                c1:45:58:28:de:ac:ca:cb:b7:f7:59:35:7f:5e:87:
                fb:3b:9d:59:02:1f:f5:26:2a:6d:ae:4d:4b:f9:8f:
                f8:89:7c:ff:8a:bb:47:55:e8:c2:76:7e:64:d8:28:
                88:02:f9:75:e3:f3:73:e9:6e:a7:90:23:89:bc:99:
                34:f2:37:65:87:cb:cc:ac:39:57:db:a7:d4:01:41:
                f8:d0:94:00:e4:f6:cb:52:52:e8:18:1f:74:2f:71:
                9e:28:d1:aa:26:2b:e7:14:e9:71:39:c0:5b:44:82:
                19:59:eb:da:44:12:d6:22:b6:1b:fe:4f:4f:af:f5:
                09:a3:9f:a7:31:d7:df:18:82:16:e2:28:d0:30:62:
                5f:48:6a:e3:b5:d8:f3:f4:68:c3:ca:27:c2:fc:53:
                92:4b:50:85:b8:c4:0a:61:49:3f:f1:4e:14:14:b0:
                d9:78:2a:50:d0:1e:84:4d:90:8f:69:d4:ee:40:14:
                1c:d2:04:80:18:be:24:84:0d:4a:61:fd:18:7f:a8:
                5c:88:5f:2a:e5:1e:1c:ab:98:1c:1a:2a:f1:b3:9c:
                49:c6:d3:c1:bc:3c:33:49:e4:81:96:89:f0:4d:6e:
                32:dd:4b:f0:d9:5b:e7:b9:b0:40:f5:10:98:68:a3:
                db:ab:ba:5a:46:9d:8c:4c:76:b3:34:aa:3b:0a:b9:
                aa:f9:86:21:26:96:cd:90:5b:8a:b7:de:93:29:62:
                53:48:6c:b0:25:70:eb:cb:d2:7c:f4:41:ac:cb:cc:
                ac:f8:8e:33:66:aa:21:b8:51:2a:52:3e:38:9d:b6:
                cf:25:b2:18:0d:13:45:a6:54:77:35:86:0b:15:f5:
                41:76:4d:61:a8:68:fd:74:f6:ec:70:47:aa:16:7e:
                f8:34:e4:15:6b:39:fa:ef:84:ae:6b:4f:98:ab:45:
                64:62:99:ee:54:b0:51:20:c4:62:cb:b8:60:96:29:
                1d:ae:84:99:19:2e:b8:c7:77:94:6a:34:8b:aa:80:
                f5:71:9a:ff:c5:5f:15:b3:bf:70:4b:b1:16:07:33:
                02:a6:31:41:af:0d:26:c0:91:95:74:83:06:78:c0:
                c2:f3:4c:ed:70:6c:f6:07:36:81:9e:cd:46:50:35:
                46:64:87:76:cd:e7:1a:e9:85:d9:fc:70:78:19:d3:
                58:1b:52:6f:3d:03:7f:24:1f:9c:43:02:fa:b7:bf:
                35:06:0f:17:02:af:d6:cd:7a:59:e7:f1:ed:91:53:
                88:a7:98:0d:2e:aa:26:33:82:b4:c2:87:21:4b:b0:
                0b:f1:23:f0:25:34:13:95:23:98:c1:fc:da:6c:1a:
                5c:31:97
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Authority Key Identifier:
            keyid:6F:1D:35:49:10:6C:32:FA:59:A0:9E:BC:8A:E8:1F:95:BE:71:7A:0C

        X509v3 Subject Key Identifier:
            7E:B3:F8:F0:37:67:05:9A:AD:2E:A9:26:D2:33:16:FB:9C:0C:18:4B
        X509v3 Key Usage: critical
            Digital Signature, Key Encipherment
        X509v3 Basic Constraints: critical
            CA:FALSE
        X509v3 Extended Key Usage:
            TLS Web Server Authentication, TLS Web Client Authentication
        X509v3 Certificate Policies:
            Policy: 1.3.6.1.4.1.6449.1.2.2.79
              CPS: https://sectigo.com/CPS
            Policy: 2.23.140.1.2.2

        X509v3 CRL Distribution Points:

            Full Name:
              URI:http://GEANT.crl.sectigo.com/GEANTOVRSACA4.crl

        Authority Information Access:
            CA Issuers - URI:http://GEANT.crt.sectigo.com/GEANTOVRSACA4.crt
            OCSP - URI:http://GEANT.ocsp.sectigo.com

        1.3.6.1.4.1.11129.2.4.2:
```

```
                ...j.h.w...V...|...[.i....qgJ......[w..;......4yC.....H0F.!...&....y.....v....>.O.f....W.....!......V
9..........."].FX....,....u...
.E....~8.GgwS..[...+^.,..P.G......4y......F0D. 1..67u;v(.........@..._..u..;.-B. av.......j=[........4`.-.K&....<.v.Nu.'\...8[1..?
R.......i...d.b.9......4x......G0E.!...d.\.d4$..Q.G..V"..../T.H.9!^... _.f.:>.....1#qF.V.K.A<2`rLCo....
            X509v3 Subject Alternative Name:
                DNS:fpsfinancesssl.minfin.fgov.be
    Signature Algorithm: sha384WithRSAEncryption
         60:58:64:1f:6b:c4:2c:2a:ef:a8:eb:c1:83:59:d4:8f:32:5c:
         d4:32:01:7f:fc:3c:ca:df:39:5f:87:9a:9e:44:0f:f7:a4:17:
         5d:cf:95:e4:0f:9e:d6:11:d5:3b:82:95:bc:28:62:9b:4d:ab:
         53:4e:21:17:3b:2b:6d:15:dd:55:98:7b:80:f1:5b:a6:07:56:
         ce:c7:02:9b:82:26:9f:26:d0:46:06:8e:5a:9c:11:93:be:67:
         48:58:21:9d:f4:d1:3f:79:e6:52:cb:b7:4d:7e:a7:bb:c9:e9:
         cf:d2:57:c1:48:a9:18:82:78:80:6a:1c:49:53:ae:d3:e0:05:
         cb:43:d6:be:a0:5b:98:0d:04:93:22:2c:30:b5:7c:2d:f8:b9:
         f7:65:28:74:a9:82:e9:a2:8e:a1:a5:82:bd:5c:76:cd:85:4b:
         ee:69:5e:f5:ce:ad:02:3d:17:1b:1c:09:ac:51:03:ae:a1:3c:
         49:f7:fd:a3:d7:96:5b:4e:c5:a1:e2:ca:d0:1b:ba:16:1c:51:
         47:97:d9:cd:31:f4:df:b8:6d:d3:8a:40:70:cf:9a:3c:51:67:
         9e:07:da:70:dd:aa:37:cc:61:d8:17:b9:45:bb:ca:0e:a9:ff:
         69:77:e0:93:89:18:3d:3b:f9:86:c9:a0:5d:ea:0a:8f:5f:54:
         38:dd:98:41:3a:56:35:32:5e:b2:d3:06:d3:e7:7e:38:6d:4f:
         e9:fc:46:98:21:18:59:3e:7c:a6:24:7f:07:d3:92:99:d5:2e:
         62:01:7c:96:af:17:c2:df:3d:5c:ec:fa:29:00:07:4b:b1:ec:
         b8:0b:7d:e6:62:91:83:d0:77:c6:e4:4d:3b:6f:ed:98:fa:68:
         51:97:e9:aa:a5:83:55:b2:eb:9e:d2:35:89:50:53:dd:d9:2d:
         a5:d0:5c:32:3c:f3:7e:f3:89:d6:09:04:14:2a:22:e4:58:91:
         18:1f:15:e3:39:c1:3a:19:a1:95:6a:2f:74:cd:bf:14:78:83:
         36:53:a9:82:5b:ea:b2:a8:22:02:99:77:77:a2:d4:23:ed:5a:
         81:10:e5:3d:c3:8a:1f:29:d4:70:26:92:28:df:57:b9:5b:a3:
         30:54:b8:a5:4b:01:98:44:6d:29:60:54:db:ef:c2:24:b2:9d:
         88:f6:2c:26:66:4d:38:79:45:2d:96:e3:4e:79:21:ab:45:f6:
         24:b9:55:94:e0:6d:e1:56:a5:1f:7e:26:1a:df:e9:27:4d:9b:
         f9:c4:69:aa:14:72:bd:13:bc:6e:07:6d:8c:d0:93:41:af:40:
         d8:b3:cd:58:5a:b3:b0:68:cb:b8:a2:fd:fa:7e:d5:89:19:c3:
         bc:ce:8e:2c:45:f3:6e:8f
-----BEGIN CERTIFICATE-----
MIIIiTCCBnGgAwIBAgIQP1nUyf4TRwPZ+Ou88ceQqzANBgkqhkiG9w0BAQwFADBE
MQswCQYDVQQGEwJOTDEZMBcGA1UEChMQR0VBTlQgVmVyZW5pZ2luZzEaMBgGA1UE
AxMRR0VBTlQgT1YgUlNBIENBIDQwHhcNMjQwNDIyMDAwMDAwWhcNMjUwNDIyMjM1
OTU5WjCBiDELMAkGA1UEBhMCQkUxJzAlBgNVBAgMHkJydXhlbGxlcy1DYXBpdGFs
ZSwgUsOpZ2lvbiBkZTEoMCYGA1UEChMfU2VydmljZSBQdWJsaWMgRmVkZXJhbCBG
aW5hbmNlczEmMCQGA1UEAxMdZnBzZmluYW5jZXNzc2wubWluZmluLmZnb3YuYmUw
ggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDJqdS3voeHszaTqM65j8FF
WCjerMrLt/dZNX9eh/s7nVkCH/UmKm2uTUv5j/iJfP+Ku0dV6MJ2fmTYKIgC+XXj
83PpbqeQI4m8mTTyN2WHy8ysOVfbp9QBQfjQlADk9stSUugYH3QvcZ4o0aomK+cU
6XE5wFtEghlZ69pEEtYithv+T0+v9Qmjn6cx198YghbiKNAwYl9IauO12PP0aMPK
J8L8U5JLUIW4xAphST/xThQUsN14KlDQHoRNkI9p1O5AFBzSBIAYviSEDUph/Rh/
qFyIXyrlHhyrmBwaKvGznEnG08G8PDNJ5IGWifBNbjLdS/DZW+e5sED1EJhoo9ur
ulpGnYxMdrM0qjsKuar5hiEmls2QW4q33pMpYlNIbLAlcOvL0nz0QazLzKz4jjNm
qiG4USpSPjidts8lshgNE0WmVHc1hgsV9UF2TWGoaP109uxwR6oWfvg05BVrOfrv
hK5rT5irRWRime5UsFEgxGLLuGCWKR2uhJkZLrjHd5RqNIuqgPVxmv/FXxWzv3BL
sRYHMwKmMUGvDSbAkZV0gwZ4wMLzTO1wbPYHNoGezUZQNUZkh3bN5xrphdn8cHgZ
01gbUm89A38kH5xDAvq3vzUGDxcCr9bNelnn8e2RU4inmA0uqiYzgrTChyFLsAvx
I/AlNBOVI5jB/NpsGlwxlwIDAQABo4IDMDCCAywwHwYDVR0jBBgwFoAUbx01SRBs
MvpZoJ68iugflb5xegwwHQYDVR0OBBYEFH6z+PA3ZwWarS6pJtIzFvucDBhLMA4G
A1UdDwEB/wQEAwIFoDAMBgNVHRMBAf8EAjAAMB0GA1UdJQQWMBQGCCsGAQUFBwMB
BggrBgEFBQcDAjBJBgNVHSAEQjBAMDQGCysGAQQBsjEBAgJPMCUwIwYIKwYBBQUH
AgEWF2h0dHBzOi8vc2VjdGlnby5jb20vQ1BTMAgGBmeBDAECAjA/BgNVHR8EODA2
MDSgMqAwhi5odHRwOi8vR0VBTlQuY3JsLnNlY3RpZ28uY29tL0dFQU5UT1ZSU0FD
QTQuY3JsMHUGCCsGAQUFBwEBBGkwZzA6BggrBgEFBQcwAoYuaHR0cDovL0dFQU5U
LmNydC5zZWN0aWdvLmNvbS9HRUFOVE9WUlNBQ0E0LmNydDApBggrBgEFBQcwAYYd
aHR0cDovL0dFQU5ULm9jc3Auc2VjdGlnby5jb20wggF+BgorBgEEAdZ5AgQCBIIB
bgSCAWoBaAB3AM8RVu7VLnyv84db2Wkum+kacWdKsBfsrAHSW3fOzDsIAAABjwU0
eUMAAAQDAEgwRgIhANTFJqn+1Zl59RMYmhx2sw4Skj7cT+VmEurXpVcG1szkAiEA
zML+7cxWOdb94sODC9eBB/YJIl2SRlgYFKLnlSz1p48AdQCi4wrkRe+9rZt+OO1H
Z3dT14JbhJTXK14bLMS5UKRH5wAAAY8FNHkGAAAEAwBGMEQCIDGDrzY3dTt2KOMQ
kbuv8sT2+UD65KpfH8B1uwM7uS1CAiBhdrMa0Amhv4hqPVvC08nYGtSzBjRg/y2L
SybDy+6iPAB2AE51oydcmhDDOFts1N8/Uusd8OCOG41pwLH6ZLFimjnfAAABjwU0
eNUAAAQDAEcwRQIhAKORZJ9cC2Q0JNmVUaNHoYRWIgGR8Y0vVAJI2DkhXuoCAiBf
BmblOj6YvO685WwjcUaNVpRLmUE8MmByTENvpJ3x2DAoBgNVHREEITAfgh1mcHNm
aW5hbmNlc3NzbC5taW5maW4uZmdvdi5iZTANBgkqhkiG9w0BAQwFAAOCAgEAYFhk
H2vELCrvqOvBg1nUjzJc1DIBf/w8yt85X4eankQP96QXXc+V5A+e1hHVO4KVvChi
m02rU04hFzsrbRXdVZh7gPFbpgdWzscCm4ImnybQRgaOWpwRk75nSFghnfTRP3nm
Usu3TX6nu8npz9JXwUipGIJ4gGocSVOu0+AFy0PWvqBbmA0EkyIsMLV8Lfi592Uo
dKmC6aKOoaWCvVx2zYVL7mle9c6tAj0XGxwJrFEDrqE8Sff9o9eWW07FoeLK0Bu6
FhxRR5fZzTH037ht04pAcM+aPFFnngfacN2qN8xh2Be5RbvKDqn/aXfgk4kYPTv5
hsmgXeoKj19UON2YQTpWNTJestMG0+d+OG1P6fxGmCEYWT58piR/B9OSmdUuYgF8
lq8Xwt89XOz6KQAHS7HsuAt95mKRg9B3xuRNO2/tmPpoUZfpqqWDVbLrntI1iVBT
3dktpdBcMjzzfvOJ1gkEFCoi5FiRGB8V4znBOhmhlWovdM2/FHiDNlOpglvqsqgi
Apl3d6LUI+1agRDlPcOKHynUcCaSKN9XuVujMFS4pUsBmERtKWBU2+/CJLKdiPYs
JmZNOHlFLZbjTnkhq0X2JLlVlOBt4ValH34mGt/pJ02b+cRpqhRyvRO8bgdtjNCT
Qa9A2LPNWFqzsGjLuKL9+n7ViRnDvM6OLEXzbo8=
-----END CERTIFICATE-----
```

Certificate ASN.1 Information

```
   0 2185: SEQUENCE {
   4 1649:   SEQUENCE {
   8    3:     [0] {
  10    1:       INTEGER 2
        :       }
  13   16:     INTEGER 3F 59 D4 C9 FE 13 47 03 D9 F8 EB BC F1 C7 90 AB
  31   13:     SEQUENCE {
```

```
 33    9:       OBJECT IDENTIFIER
       :         sha384WithRSAEncryption (1 2 840 113549 1 1 12)
 44    0:       NULL
       :       }
 46   68:     SEQUENCE {
 48   11:       SET {
 50    9:         SEQUENCE {
 52    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 57    2:           PrintableString 'NL'
       :           }
       :         }
 61   25:       SET {
 63   23:         SEQUENCE {
 65    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 70   16:           PrintableString 'GEANT Vereniging'
       :           }
       :         }
 88   26:       SET {
 90   24:         SEQUENCE {
 92    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
 97   17:           PrintableString 'GEANT OV RSA CA 4'
       :           }
       :         }
       :       }
116   30:     SEQUENCE {
118   13:       UTCTime 22/04/2024 00:00:00 GMT
133   13:       UTCTime 22/04/2025 23:59:59 GMT
       :       }
148  136:     SEQUENCE {
151   11:       SET {
153    9:         SEQUENCE {
155    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
160    2:           PrintableString 'BE'
       :           }
       :         }
164   39:       SET {
166   37:         SEQUENCE {
168    3:           OBJECT IDENTIFIER stateOrProvinceName (2 5 4 8)
173   30:           UTF8String 'Bruxelles-Capitale, R..gion de'
       :           }
       :         }
205   40:       SET {
207   38:         SEQUENCE {
209    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
214   31:           PrintableString 'Service Public Federal Finances'
       :           }
       :         }
247   38:       SET {
249   36:         SEQUENCE {
251    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
256   29:           PrintableString 'fpsfinancesssl.minfin.fgov.be'
       :           }
       :         }
       :       }
287  546:     SEQUENCE {
291   13:       SEQUENCE {
293    9:         OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
304    0:         NULL
       :         }
306  527:       BIT STRING
       :         30 82 02 0A 02 82 02 01 00 C9 A9 D4 B7 BE 87 87
       :         B3 36 93 A8 CE B9 8F C1 45 58 28 DE AC CA CB B7
       :         F7 59 35 7F 5E 87 FB 3B 9D 59 02 1F F5 26 2A 6D
       :         AE 4D 4B F9 8F F8 89 7C FF 8A BB 47 55 E8 C2 76
       :         7E 64 D8 28 88 02 F9 75 E3 F3 73 E9 6E A7 90 23
       :         89 BC 99 34 F2 37 65 87 CB CC AC 39 57 DB A7 D4
       :         01 41 F8 D0 94 00 E4 F6 CB 52 52 E8 18 1F 74 2F
       :         71 9E 28 D1 AA 26 2B E7 14 E9 71 39 C0 5B 44 82
       :                 [ Another 398 bytes skipped ]
       :       }
837  816:     [3] {
841  812:       SEQUENCE {
845   31:         SEQUENCE {
847    3:           OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
852   24:           OCTET STRING
       :             30 16 80 14 6F 1D 35 49 10 6C 32 FA 59 A0 9E BC
       :             8A E8 1F 95 BE 71 7A 0C
       :           }
878   29:         SEQUENCE {
880    3:           OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
885   22:           OCTET STRING
       :             04 14 7E B3 F8 F0 37 67 05 9A AD 2E A9 26 D2 33
       :             16 FB 9C 0C 18 4B
       :           }
909   14:         SEQUENCE {
911    3:           OBJECT IDENTIFIER keyUsage (2 5 29 15)
916    1:           BOOLEAN TRUE
919    4:           OCTET STRING 03 02 05 A0
       :           }
925   12:         SEQUENCE {
927    3:           OBJECT IDENTIFIER basicConstraints (2 5 29 19)
932    1:           BOOLEAN TRUE
935    2:           OCTET STRING 30 00
       :           }
939   29:         SEQUENCE {
941    3:           OBJECT IDENTIFIER extKeyUsage (2 5 29 37)
946   22:           OCTET STRING
```

```
         :             30 14 06 08 2B 06 01 05 05 07 03 01 06 08 2B 06
         :             01 05 05 07 03 02
         :           }
 970   73:         SEQUENCE {
 972    3:           OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
 977   66:           OCTET STRING
         :             30 40 30 34 06 0B 2B 06 01 04 01 B2 31 01 02 02
         :             4F 30 25 30 23 06 08 2B 06 01 05 05 07 02 01 16
         :             17 68 74 74 70 73 3A 2F 2F 73 65 63 74 69 67 6F
         :             2E 63 6F 6D 2F 43 50 53 30 08 06 06 67 81 0C 01
         :             02 02
         :           }
1045   63:         SEQUENCE {
1047    3:           OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
1052   56:           OCTET STRING
         :             30 36 30 34 A0 32 A0 30 86 2E 68 74 74 70 3A 2F
         :             2F 47 45 41 4E 54 2E 63 72 6C 2E 73 65 63 74 69
         :             67 6F 2E 63 6F 6D 2F 47 45 41 4E 54 4F 56 52 53
         :             41 43 41 34 2E 63 72 6C
         :           }
1110  117:         SEQUENCE {
1112    8:           OBJECT IDENTIFIER authorityInfoAccess (1 3 6 1 5 5 7 1 1)
1122  105:           OCTET STRING
         :             30 67 30 3A 06 08 2B 06 01 05 05 07 30 02 86 2E
         :             68 74 74 70 3A 2F 2F 47 45 41 4E 54 2E 63 72 74
         :             2E 73 65 63 74 69 67 6F 2E 63 6F 6D 2F 47 45 41
         :             4E 54 4F 56 52 53 41 43 41 34 2E 63 72 74 30 29
         :             06 08 2B 06 01 05 05 07 30 01 86 1D 68 74 74 70
         :             3A 2F 2F 47 45 41 4E 54 2E 6F 63 73 70 2E 73 65
         :             63 74 69 67 6F 2E 63 6F 6D
         :           }
1229  382:         SEQUENCE {
1233   10:           OBJECT IDENTIFIER '1 3 6 1 4 1 11129 2 4 2'
1245  366:           OCTET STRING
         :             04 82 01 6A 01 68 00 77 00 CF 11 56 EE D5 2E 7C
         :             AF F3 87 5B D9 69 2E 9B E9 1A 71 67 4A B0 17 EC
         :             AC 01 D2 5B 77 CE CC 3B 08 00 00 01 8F 05 34 79
         :             43 00 00 04 03 00 48 30 46 02 21 00 D4 C5 26 A9
         :             FE D5 99 79 F5 13 18 9A 1C 76 B3 0E 12 92 3E DC
         :             4F E5 66 12 EA D7 A5 57 06 D6 CC E4 02 21 00 CC
         :             C2 FE ED CC 56 39 D6 FD E2 C3 83 0B D7 81 07 F6
         :             09 22 5D 92 46 58 18 14 A2 E7 95 2C F5 A7 8F 00
         :                     [ Another 238 bytes skipped ]
         :           }
1615   40:         SEQUENCE {
1617    3:           OBJECT IDENTIFIER subjectAltName (2 5 29 17)
1622   33:           OCTET STRING
         :             30 1F 82 1D 66 70 73 66 69 6E 61 6E 63 65 73 73
         :             73 6C 2E 6D 69 6E 66 69 6E 2E 66 67 6F 76 2E 62
         :             65
         :           }
         :         }
         :       }
         :     }
1657   13:   SEQUENCE {
1659    9:     OBJECT IDENTIFIER sha384WithRSAEncryption (1 2 840 113549 1 1 12)
1670    0:     NULL
         :     }
1672  513:   BIT STRING
         :     60 58 64 1F 6B C4 2C 2A EF A8 EB C1 83 59 D4 8F
         :     32 5C D4 32 01 7F FC 3C CA DF 39 5F 87 9A 9E 44
         :     0F F7 A4 17 5D CF 95 E4 0F 9E D6 11 D5 3B 82 95
         :     BC 28 62 9B 4D AB 53 4E 21 17 3B 2B 6D 15 DD 55
         :     98 7B 80 F1 5B A6 07 56 CE C7 02 9B 82 26 9F 26
         :     D0 46 06 8E 5A 9C 11 93 BE 67 48 58 21 9D F4 D1
         :     3F 79 E6 52 CB B7 4D 7E A7 BB C9 E9 CF D2 57 C1
         :     48 A9 18 82 78 80 6A 1C 49 53 AE D3 E0 05 CB 43
         :             [ Another 384 bytes skipped ]
         :   }
```