CSR Decoder and Certificate Decoder

```
-----BEGIN CERTIFICATE REQUEST-----
MIICrjCCAZYCAQAwaTELMAkGA1UEBgwCVVMxITAfBgNVBAoMGENlcnRpZmljYXRl
IFRlc3QgUGFydG5lcjEhMB8GA1UECwwYQ2VydGlmaWNhdGUgVGVzdCBQYXJ0bmVy
MRQwEgYDVQQDDAtKdXN0aW4gVGVzdDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAKYhmsGuY15fv1z8Zg7AmqNGxvwsY1w/DjgYC26x1JZZm3JOkFnPI/AM
CrcegwzWHyA4oX/S+Ng97b/F9sL/9bhDSqyCGC1qSsizu3drdsCfXQFg7ahTmIY8
xZdNvOMo0AM+i0AZS/oCgkbASFMIK3VpDTbQhJqdZ1AeP6RjV+XpwfrpQsxFiN9H
ZU/mFkBb0Mf0enUejHwLmhjVMrjRjzwpF58cMgwRgJKvDvtgLFls7ZPmDDBv/iEK
NcVq7Puv3Z+J/lOTw6el1Md7H2qhcN6F+3GnMVsn31zLGLrG94NcXkX1/8zjP8GW
/6uWnJzztwzOPIpTSyRVTwFybl+XtQUCAwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IB
AQCiMCBVbFJ0xs+pl5dNAHVG5xSiqsMs280K66IRvVpXpwhrwbkL3kfv6so9gIs/
myLYGRxYulgkz1XrHhV4Sa0giO1Qab6KKy7UWzQEX5bLCBwZLKJoRO7KCkfEXjdw
vyJs8F8fASkcHAqj3dFZgF9jmxRaRlqvmWpIXDtuaZXyl2lqvBfU42GUM554FPsN
Au5FJl/bLeEGA5dE76iKuA7IXmifb4qHyMfLD6nDNxIvYGadbOxm12xpN0xAeWIE
nKJNKYYlI5Qc4YS2uQXbUOITIEvWtAoFunKKLFQkHeaXMR8eRV85gj9+iRlTIJx8
S6D8PP87lwcK/7ld6Q+9o9Cb
```

Or Choose File...

Decode

CSR Summary

CSR Checks

Check	Result
Debian Weak Key	PASSED - Does not use a key on our blacklist - this is good
Key Size	PASSED (2048 bits)
Signature	FAILED - CSR has an invalid signature
MD5	PASSED - Not using the MD5 algorithm

CSR Subject

Common Name (CN)	Justin Test
Organizational Unit (OU)	Certificate Test Partner
Organization (O)	Certificate Test Partner
Country (C)	US

CSR Properties

Subject	C=US, O=Certificate Test Partner, OU=Certificate Test Partner, CN=Justin Test
Key Size	2048 bits
Key Algorithm	RSA
Sig. Algorithm	sha256WithRSAEncryption
SHA256 Fingerprint	40:C0:26:C8:DA:CA:75:25:68:16:A6:50:F3:D1:C6:48:F6:C5:66:9F:55:5B:1C:6C:6F:BF:AD:A0:80:0E:3D:10
SHA1 Fingerprint	BE:4E:DB:9E:69:03:77:57:AB:F3:01:80:6C:26:63:70:36:AE:41:BC

MD5 Fingeprint	9E:6A:CF:BC:AE:C4:F3:35:0C:FD:4F:0E:A7:FA:D2:9E
SANS	

CSR Detailed Information

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=US, O=Certificate Test Partner, OU=Certificate Test Partner, CN=Justin Test
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a6:21:9a:c1:ae:63:5e:5f:bf:5c:fc:66:0e:c0:
                    9a:a3:46:c6:fc:2c:63:5c:3f:0e:38:18:0b:6e:b1:
                    d4:96:59:9b:72:4e:90:59:cf:23:f0:0c:0a:b7:1e:
                    83:0c:d6:1f:20:38:a1:7f:d2:f8:d8:3d:ed:bf:c5:
                    f6:c2:ff:f5:b8:43:4a:ac:82:18:2d:6a:4a:c8:b3:
                    bb:77:6b:76:c0:9f:5d:01:60:ed:a8:53:98:86:3c:
                    c5:97:4d:bc:e3:28:d0:03:3e:8b:40:19:4b:fa:02:
                    82:46:c0:48:53:08:2b:75:69:0d:36:d0:84:9a:9d:
                    67:50:1e:3f:a4:63:57:e5:e9:c1:fa:e9:42:cc:45:
                    88:df:47:65:4f:e6:16:40:5b:d0:c7:f4:7a:75:1e:
                    8c:7c:0b:9a:18:d5:32:b8:d1:8f:3c:29:17:9f:1c:
                    32:0c:11:80:92:af:0e:fb:60:2c:59:6c:ed:93:e6:
                    0c:30:6f:fe:21:0a:35:c5:6a:ec:fb:af:dd:9f:89:
                    fe:53:93:c3:a7:a5:d4:c7:7b:1f:6a:a1:70:de:85:
                    fb:71:a7:31:5b:27:df:5c:cb:18:ba:c6:f7:83:5c:
                    5e:45:f5:ff:cc:e3:3f:c1:96:ff:ab:96:9c:9c:f3:
                    b7:0c:ce:3c:8a:53:4b:24:55:4f:01:72:6e:5f:97:
                    b5:05
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         a2:30:20:55:6c:52:74:c6:cf:a9:97:97:4d:00:75:46:e7:14:
         a2:aa:c3:2c:db:cd:0a:eb:a2:11:bd:5a:57:a7:08:6b:c1:b9:
         0b:de:47:ef:ea:ca:3d:80:8b:3f:9b:22:d8:19:1c:58:ba:58:
         24:cf:55:eb:1e:15:78:49:ad:20:88:ed:50:69:be:8a:2b:2e:
         d4:5b:34:04:5f:96:cb:08:1c:19:2c:a2:68:44:ee:ca:0a:47:
         c4:5e:37:70:bf:22:6c:f0:5f:1f:01:29:1c:1c:0a:a3:dd:d1:
         59:80:5f:63:9b:14:5a:46:5a:af:99:6a:48:5c:3b:6e:69:95:
         f2:97:69:6a:bc:17:d4:e3:61:94:33:9e:78:14:fb:0d:02:ee:
         45:26:5f:db:2d:e1:06:03:97:44:ef:a8:8a:b8:0e:c8:5e:68:
         9f:6f:8a:87:c8:c7:cb:0f:a9:c3:37:12:2f:60:66:9d:6c:ec:
         66:d7:6c:69:37:4c:40:79:62:04:9c:a2:4d:29:86:25:23:94:
         1c:e1:84:b6:b9:05:db:50:e2:13:20:4b:d6:b4:0a:05:ba:72:
         8a:2c:54:24:1d:e6:97:31:1f:1e:45:5f:39:82:3f:7e:89:19:
         53:20:9c:7c:4b:a0:fc:3c:ff:3b:97:07:0a:ff:b9:5d:e9:0f:
         bd:a3:d0:9b
```

CSR ASN.1 Information

```
  0 686: SEQUENCE {
  4 406:   SEQUENCE {
  8   1:     INTEGER 0
 11 105:     SEQUENCE {
 13  11:       SET {
 15   9:         SEQUENCE {
 17   3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 22   2:           UTF8String 'US'
       :           }
       :         }
 26  33:       SET {
 28  31:         SEQUENCE {
 30   3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 35  24:           UTF8String 'Certificate Test Partner'
       :           }
       :         }
 61  33:       SET {
 63  31:         SEQUENCE {
 65   3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
 70  24:           UTF8String 'Certificate Test Partner'
       :           }
       :         }
 96  20:       SET {
 98  18:         SEQUENCE {
100   3:           OBJECT IDENTIFIER commonName (2 5 4 3)
105  11:           UTF8String 'Justin Test'
       :           }
       :         }
       :       }
118 290:     SEQUENCE {
122  13:       SEQUENCE {
124   9:         OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
135   0:         NULL
       :         }
137 271:       BIT STRING
       :         30 82 01 0A 02 82 01 01 00 A6 21 9A C1 AE 63 5E
       :         5F BF 5C FC 66 0E C0 9A A3 46 C6 FC 2C 63 5C 3F
       :         0E 38 18 0B 6E B1 D4 96 59 9B 72 4E 90 59 CF 23
       :         F0 0C 0A B7 1E 83 0C D6 1F 20 38 A1 7F D2 F8 D8
       :         3D ED BF C5 F6 C2 FF F5 B8 43 4A AC 82 18 2D 6A
       :         4A C8 B3 BB 77 6B 76 C0 9F 5D 01 60 ED A8 53 98
       :         86 3C C5 97 4D BC E3 28 D0 03 3E 8B 40 19 4B FA
       :         02 82 46 C0 48 53 08 2B 75 69 0D 36 D0 84 9A 9D
       :                 [ Another 142 bytes skipped ]
       :       }
412   0:     [0]
       :       Error: Object has zero length.
       :     }
414  13:   SEQUENCE {
416   9:     OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
427   0:     NULL
       :     }
429 257:   BIT STRING
       :     A2 30 20 55 6C 52 74 C6 CF A9 97 97 4D 00 75 46
       :     E7 14 A2 AA C3 2C DB CD 0A EB A2 11 BD 5A 57 A7
       :     08 6B C1 B9 0B DE 47 EF EA CA 3D 80 8B 3F 9B 22
       :     D8 19 1C 58 BA 58 24 CF 55 EB 1E 15 78 49 AD 20
       :     88 ED 50 69 BE 8A 2B 2E D4 5B 34 04 5F 96 CB 08
       :     1C 19 2C A2 68 44 EE CA 0A 47 C4 5E 37 70 BF 22
       :     6C F0 5F 1F 01 29 1C 1C 0A A3 DD D1 59 80 5F 63
       :     9B 14 5A 46 5A AF 99 6A 48 5C 3B 6E 69 95 F2 97
       :             [ Another 128 bytes skipped ]
       :   }
```

CSR Hex Encoded

```
308202ae308201960201003069310b300906035504060c0255533121301f0603
55040a0c184365727469666963617465205465737420506172746e6572312130
1f060355040b0c184365727469666963617465205465737420506172746e6572
311430120603550403 0c0b4a757374696e20546573743082012300d06092a86
4886f70d0101010500038201 0f003082010a0282010100a6219ac1ae635e5fbf
5cfc660ec09aa346c6fc2c635c3f0e38180b6eb1d496599b724e9059cf23f00c
0ab71e830cd61f2038a17fd2f8d83dedbfc5f6c2fff5b8434aac82182d6a4ac8
b3bb776b76c09f5d0160eda85398863cc5974dbce328d0033e8b40194bfa0282
46c04853082b75690d36d0849a9d67501e3fa46357e5e9c1fae942cc4588df47
654fe616405bd0c7f47a751e8c7c0b9a18d532b8d18f3c29179f1c320c118092
af0efb602c596ced93e60c306ffe210a35c56aecfbafdd9f89fe5393c3a7a5d4
c77b1f6aa170de85fb71a7315b27df5ccb18bac6f7835c5e45f5ffcce33fc196
ffab969c9cf3b70cce3c8a534b24554f01726e5f97b5050203010001a000300d
06092a864886f70d01010b05000382010100a23020556c5274c6cfa997974d00
7546e714a2aac32cdbcd0aeba211bd5a57a7086bc1b90bde47efeaca3d808b3f
9b22d8191c58ba5824cf55eb1e157849ad2088ed5069be8a2b2ed45b34045f96
cb081c192ca26844eeca0a47c45e3770bf226cf05f1f01291c1c0aa3ddd15980
5f639b145a465aaf996a485c3b6e6995f297696abc17d4e36194339e7814fb0d
02ee45265fdb2de106039744efa88ab80ec85e689f6f8a87c8c7cb0fa9c33712
2f60669d6cec66d76c69374c407962049ca24d29862523941ce184b6b905db50
e213204bd6b40a05ba728a2c54241de697311f1e455f39823f7e891953209c7c
4ba0fc3cff3b97070affb95de90fbda3d09b
```