Secure Communications

Week 9

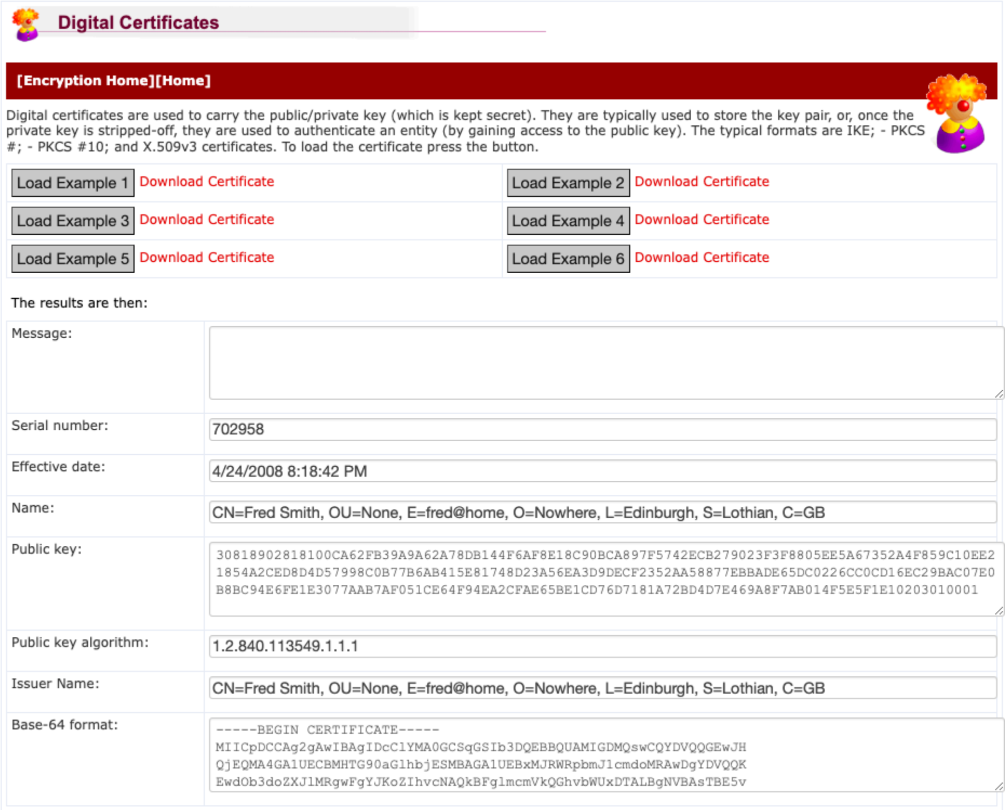
Trust and Digital Certificates

Sections

A. Introduction

A.1 http://asecuritysite.com/encryption/digitalcert

Certificate 1



Digital Certificates
[Encryption Home][Home]

Digital certificates are used to carry the public/private key (which is kept secret). They are typically used to store the key pair, or, once the private key is stripped-off, they are used to authenticate an entity (by gaining access to the public key). The typical formats are IKE; - PKCS #; - PKCS #10; and X.509v3 certificates. To load the certificate press the button.

Load Example 1 Download Certificate
Load Example 2 Download Certificate
Load Example 3 Download Certificate
Load Example 4 Download Certificate
Load Example 5 Download Certificate
Load Example 6 Download Certificate

The results are then:

Message:

Serial number: 702958

Effective date: 4/24/2008 8:18:42 PM

Name: CN=Fred Smith, OU=None, E=fred@home, O=Nowhere, L=Edinburgh, S=Lothian, C=GB

Public key:

```
30818902818100CA62FB39A9A62A78DB144F6AF8E18C90BCA897F5742ECB279023F3F8805EE5A67352A4F859C10EE2
1854A2CED8D4D57998C0B77B6AB415E81748D23A56EA3D9DECF2352AA58877EBBADE65DC0226CC0CD16EC29BAC07E0
B8BC94E6FE1E3077AAB7AF051CE64F94EA2CFAE65BE1CD76D7181A72BD4D7E469A8F7AB014F5E5F1E10203010001
```

Public key algorithm: 1.2.840.113549.1.1.1

Issuer Name: CN=Fred Smith, OU=None, E=fred@home, O=Nowhere, L=Edinburgh, S=Lothian, C=GB

Base-64 format:

```
-----BEGIN CERTIFICATE-----
MIICpDCCAg2gAwIBAgIDcClYMA0GCSqGSIb3DQEBBQUAMIGDMQswCQYDVQQGEwJH
QjEQMA4GA1UECBMHTG90aGlhbjESMBAGA1UEBxMJRWRpbmJ1cmdoMRAwDgYDVQQK
EwdOb3doZXJlMRgwFgYJKoZIhvcNAQkBFglmcmVkQGhvbWUxDTALBgNVBAsTBE5v
```

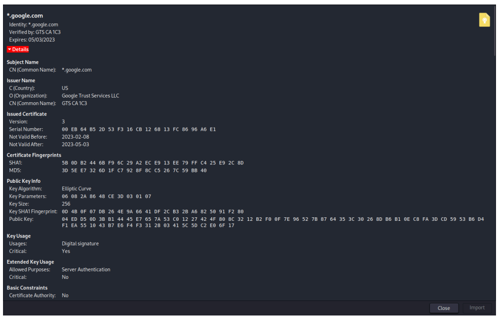
Serial number:	702958
Effective date:	4/24/2008 8:18:42 PM
Name:	CN=Fred Smith, OU=None, E=fred@home, O=Nowhere, L=Edinburgh, S=Lothian, C=GB
Issuer:	CN=Fred Smith, OU=None, E=fred@home, O=Nowhere, L=Edinburgh, S=Lothian, C=GB
What is CN used	The Common Name – the primary name of the certificate

for:	holder, typically the domain name or person's name
What is ON used for:	Organizational Unit – identifies the department or group within the organization
What is O used for:	Organization – the company or legal entity owning the certificate
What is L used for:	Locality – the city where the organization or certificate owner is located

A.2 `openssl x509 -inform der -in [filename].der -noout -text`

`openssl verify google.cer`

Certificate 3



*.google.com
Identity: *.google.com
Verified by: GTS CA 1C3
Expires: 05/03/2023

▾ Details

Subject Name

CN (Common Name):	*.google.com

Issuer Name

C (Country):	US
O (Organization):	Google Trust Services LLC
CN (Common Name):	GTS CA 1C3

Issued Certificate

Version:	3
Serial Number:	00 EB 64 B5 2D 53 F3 16 CB 12 68 13 FC 86 96 A6 E1
Not Valid Before:	2023-02-08
Not Valid After:	2023-05-03

Certificate Fingerprints

SHA1:	5B 0D B2 44 6B F9 6C 29 A2 EC E9 13 EE 79 FF C4 25 E9 2C 8D
MD5:	3D 5E E7 32 6D 1F C7 92 8F 8C C5 26 7C 59 BB 40

Public Key Info

Key Algorithm:	Elliptic Curve
Key Parameters:	06 08 2A 86 48 CE 3D 03 01 07
Key Size:	256
Key SHA1 Fingerprint:	0D 4B 0F 07 DB 26 4E 9A 66 41 DF 2C B3 2B A6 82 50 91 F2 80
Public Key:	04 ED D5 0D 3B B1 44 45 E7 65 7A 53 C0 12 27 42 4F 80 8C 32 12 B2 F0 0F 7E 96 52 7B 87 64 35 3C 30 26 8D B6 B1 0E C8 FA 3D CD 59 53 B6 D4 F1 EA 55 10 43 B7 E6 F4 F3 31 28 03 41 5C 5D C2 E0 6F 17

Key Usage

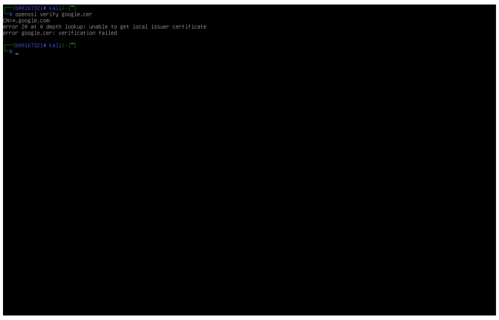
Usages:	Digital signature
Critical:	Yes

Extended Key Usage

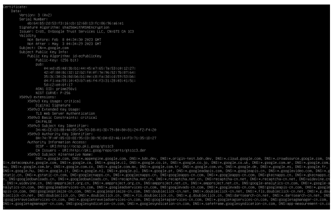
Allowed Purposes:	Server Authentication
Critical:	No

Basic Constraints

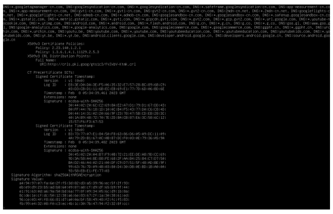
Certificate Authority:	No



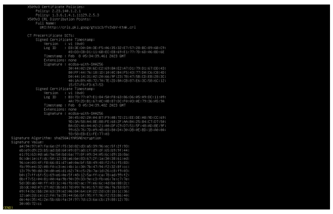
```
┌──(b00167321♦ kali)-[~]
└─$ openssl verify google.cer
CN=*.google.com
error 20 at 0 depth lookup: unable to get local issuer certificate
error google.cer: verification failed

┌──(b00167321♦ kali)-[~]
└─$ _
```



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            eb:64:b5:2d:53:f3:16:cb:12:68:13:fc:86:96:a6:e1
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Google Trust Services LLC, CN=GTS CA 1C3
        Validity
            Not Before: Feb  8 04:34:30 2023 GMT
            Not After : May  3 04:34:29 2023 GMT
        Subject: CN=*.google.com
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:ed:d5:0d:3b:b1:44:45:e7:65:7a:53:c0:12:27:
                    42:4f:80:8c:32:12:b2:f0:0f:7e:96:52:7b:87:64:
                    35:3c:30:26:8d:b6:b1:0e:c8:fa:3d:cd:59:53:b6:
                    d4:f1:ea:55:10:43:b7:e6:f4:f3:31:28:03:41:5c:
                    5d:c2:e0:6f:17
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Key Identifier:
                34:46:CE:D3:8B:4A:B5:5A:93:D8:01:3D:79:80:80:81:24:F2:F4:20
            X509v3 Authority Key Identifier:
                8A:74:7F:AF:85:CD:EE:95:CD:3D:9C:D0:E2:46:14:F3:71:35:1D:27
            Authority Information Access:
                OCSP - URI:http://ocsp.pki.goog/gts1c3
                CA Issuers - URI:http://pki.goog/repo/certs/gts1c3.der
            X509v3 Subject Alternative Name:
                DNS:*.google.com, DNS:*.appengine.google.com, DNS:*.bdn.dev, DNS:*.origin-test.bdn.dev, DNS:*.cloud.google.com, DNS:*.crowdsource.google.com, DN
S:*.datacompute.google.com, DNS:*.google.ca, DNS:*.google.cl, DNS:*.google.co.in, DNS:*.google.co.jp, DNS:*.google.co.uk, DNS:*.google.com.ar, DNS:*.google.com.
au, DNS:*.google.com.br, DNS:*.google.com.co, DNS:*.google.com.mx, DNS:*.google.com.tr, DNS:*.google.com.vn, DNS:*.google.de, DNS:*.google.es, DNS:*.google.fr,
DNS:*.google.hu, DNS:*.google.it, DNS:*.google.nl, DNS:*.google.pl, DNS:*.google.pt, DNS:*.googleadapis.com, DNS:*.googleapis.cn, DNS:*.googlevideo.com, DNS:*.g
static.cn, DNS:*.gstatic-cn.com, DNS:googlecnapps.cn, DNS:*.googlecnapps.cn, DNS:googleapps-cn.com, DNS:*.googleapps-cn.com, DNS:gkecnapps.cn, DNS:*.gkecnapps.c
n, DNS:googledownloads.cn, DNS:*.googledownloads.cn, DNS:recaptcha.net.cn, DNS:*.recaptcha.net.cn, DNS:recaptcha-cn.net, DNS:*.recaptcha-cn.net, DNS:widevine.cn
, DNS:*.widevine.cn, DNS:ampproject.org.cn, DNS:*.ampproject.org.cn, DNS:ampproject.net.cn, DNS:*.ampproject.net.cn, DNS:google-analytics-cn.com, DNS:*.google-a
nalytics-cn.com, DNS:googleadservices-cn.com, DNS:*.googleadservices-cn.com, DNS:googlevads-cn.com, DNS:*.googlevads-cn.com, DNS:googleapis-cn.com, DNS:*.google
apis-cn.com, DNS:googleoptimize-cn.com, DNS:*.googleoptimize-cn.com, DNS:doubleclick-cn.net, DNS:*.doubleclick-cn.net, DNS:*.fls.doubleclick-cn.net, DNS:*.g.dou
bleclick-cn.net, DNS:doubleclick.cn, DNS:*.doubleclick.cn, DNS:*.fls.doubleclick.cn, DNS:*.g.doubleclick.cn, DNS:dartsearch-cn.net, DNS:*.dartsearch-cn.net, DNS
:googletraveladservices-cn.com, DNS:*.googletraveladservices-cn.com, DNS:googletagservices-cn.com, DNS:*.googletagservices-cn.com, DNS:googletagmanager-cn.com,
DNS:*.googletagmanager-cn.com, DNS:googlesyndication-cn.com, DNS:*.googlesyndication-cn.com, DNS:*.safeframe.googlesyndication-cn.com, DNS:app-measurement-cn.co
:
```



```
DNS:*.googletagmanager-cn.com, DNS:googlesyndication-cn.com, DNS:*.googlesyndication-cn.com, DNS:*.safeframe.googlesyndication-cn.com, DNS:app-measurement-cn.co
m, DNS:*.app-measurement-cn.com, DNS:gvt1-cn.com, DNS:*.gvt1-cn.com, DNS:gvt2-cn.com, DNS:*.gvt2-cn.com, DNS:2mdn-cn.net, DNS:*.2mdn-cn.net, DNS:googleflights-c
n.net, DNS:*.googleflights-cn.net, DNS:admob-cn.com, DNS:*.admob-cn.com, DNS:googlesandbox-cn.com, DNS:*.googlesandbox-cn.com, DNS:*.safenup.googlesandbox-cn.co
m, DNS:*.gstatic.com, DNS:*.metric.gstatic.com, DNS:*.gvt1.com, DNS:*.gcpcdn.gvt1.com, DNS:*.gvt2.com, DNS:*.gcp.gvt2.com, DNS:*.url.google.com, DNS:*.youtube-n
ocookie.com, DNS:*.ytimg.com, DNS:android.com, DNS:*.android.com, DNS:*.flash.android.com, DNS:g.cn, DNS:*.g.cn, DNS:g.co, DNS:*.g.co, DNS:goo.gl, DNS:www.goo.g
l, DNS:google-analytics.com, DNS:*.google-analytics.com, DNS:google.com, DNS:googlecommerce.com, DNS:*.googlecommerce.com, DNS:ggpht.cn, DNS:*.ggpht.cn, DNS:urc
hin.com, DNS:*.urchin.com, DNS:youtu.be, DNS:youtube.com, DNS:*.youtube.com, DNS:youtubeeducation.com, DNS:*.youtubeeducation.com, DNS:youtubekids.com, DNS:*.yo
utubekids.com, DNS:yt.be, DNS:*.yt.be, DNS:android.clients.google.com, DNS:developer.android.google.cn, DNS:developers.android.google.cn, DNS:source.android.goo
gle.cn
            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.1
                Policy: 1.3.6.1.4.1.11129.2.5.3
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crls.pki.goog/gts1c3/fVJxbV-Ktmk.crl

            CT Precertificate SCTs:
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : E8:3E:D0:DA:3E:F5:06:35:32:E7:57:28:BC:89:6B:C9:
                                03:D3:CB:D1:11:6B:EC:EB:69:E1:77:7D:6D:06:BD:6E
                    Timestamp : Feb  8 05:34:39.461 2023 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:44:02:20:6C:C2:69:8A:E2:A7:D1:79:D1:67:DD:43:
                                B0:FF:44:76:18:1D:10:0C:B4:F5:43:77:D0:C6:C8:4D:
                                D0:44:14:31:02:20:66:9F:23:78:47:5B:CD:EB:28:3C:
                                40:1A:B9:48:72:70:7E:2D:8A:CB:87:E6:3C:58:6C:12:
                                15:57:F6:F3:67:53
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : B3:73:77:07:E1:84:50:F8:63:86:D6:05:A9:DC:11:09:
                                4A:79:2D:B1:67:0C:0B:87:DC:F0:03:0E:79:36:A5:9A
                    Timestamp : Feb  8 05:34:39.482 2023 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:45:02:20:04:B7:F9:0B:72:21:EE:DE:A8:9D:CC:69:
                                9D:3A:58:A4:8E:88:FE:68:2F:AA:B4:25:84:C7:D7:50:
                                BA:D2:46:A4:02:21:00:DF:C9:D7:51:5F:48:AD:BE:9F:
                                99:63:76:7D:09:4B:03:80:D4:30:DB:0E:BD:1B:A0:0A:
                                93:58:EB:E1:FE:77:03
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        a4:94:97:07:fa:6e:2f:f5:3d:82:d3:a5:39:96:ec:5f:2f:93:
        eb:e9:d9:23:b5:ad:b8:60:09:87:a8:cf:d9:df:65:b9:9f:44:
        e1:91:63:0d:a6:9a:50:bd:6a:77:8f:09:34:05:6c:d9:1b:8a:
        8c:de:1e:cf:dc:50:12:38:a6:6e:83:67:2f:1a:30:38:61:ed:
        96:ce:03:4f:f8:66:81:d7:a0:0a:bf:58:49:48:f2:fc:f5:83:
        fb:99:e4:32:08:f0:c3:ec:4b:1c:30:7b:47:94:f2:32:8f:cc:
:
```

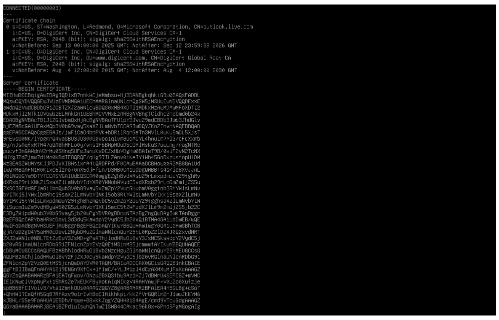


```
            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.1
                Policy: 1.3.6.1.4.1.11129.2.5.3
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crls.pki.goog/gts1c3/fVJxbV-Ktmk.crl

            CT Precertificate SCTs:
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : E8:3E:D0:DA:3E:F5:06:35:32:E7:57:28:BC:89:6B:C9:
                                03:D3:CB:D1:11:6B:EC:EB:69:E1:77:7D:6D:06:BD:6E
                    Timestamp : Feb  8 05:34:39.461 2023 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:44:02:20:6C:C2:69:8A:E2:A7:D1:79:D1:67:DD:43:
                                B0:FF:44:76:18:1D:10:0C:B4:F5:43:77:D0:C6:C8:4D:
                                D0:44:14:31:02:20:66:9F:23:78:47:5B:CD:EB:28:3C:
                                40:1A:B9:48:72:70:7E:2D:8A:CB:87:E6:3C:58:6C:12:
                                15:57:F6:F3:67:53
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : B3:73:77:07:E1:84:50:F8:63:86:D6:05:A9:DC:11:09:
                                4A:79:2D:B1:67:0C:0B:87:DC:F0:03:0E:79:36:A5:9A
                    Timestamp : Feb  8 05:34:39.482 2023 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:45:02:20:04:B7:F9:0B:72:21:EE:DE:A8:9D:CC:69:
                                9D:3A:58:A4:8E:88:FE:68:2F:AA:B4:25:84:C7:D7:50:
                                BA:D2:46:A4:02:21:00:DF:C9:D7:51:5F:48:AD:BE:9F:
                                99:63:76:7D:09:4B:03:80:D4:30:DB:0E:BD:1B:A0:0A:
                                93:58:EB:E1:FE:77:03
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        a4:94:97:07:fa:6e:2f:f5:3d:82:d3:a5:39:96:ec:5f:2f:93:
        eb:e9:d9:23:b5:ad:b8:60:09:87:a8:cf:d9:df:65:b9:9f:44:
        e1:91:63:0d:a6:9a:50:bd:6a:77:8f:09:34:05:6c:d9:1b:8a:
        8c:de:1e:cf:dc:50:12:38:a6:6e:83:67:2f:1a:30:38:61:ed:
        96:ce:03:4f:f8:66:81:d7:a0:0a:bf:58:49:48:f2:fc:f5:83:
        fb:99:e4:32:08:f0:c3:ec:4b:1c:30:7b:47:94:f2:32:8f:cc:
```

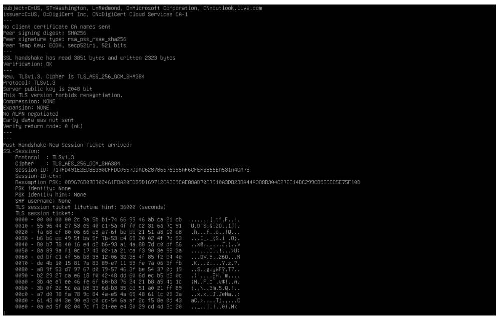
```
        13:79:98:dd:20:d0:e6:d1:62:74:c5:2b:7a:1d:26:c8:f9:03:
        b0:17:ff:6f:51:69:e6:0e:5f:48:12:5a:ff:ca:78:ad:99:f2:
        8b:f7:51:04:81:00:4a:9b:90:39:33:9e:c3:fb:e6:7e:c7:7e:
        5d:38:ab:40:ff:43:1c:46:fb:02:ac:7f:e6:6c:4d:be:88:2c:
        1b:dc:0d:07:27:02:3b:e3:7d:09:7e:01:57:82:06:76:53:b7:
        09:f4:bc:bb:20:63:39:e2:06:04:64:c0:22:2d:c8:1b:1c:36:
        12:a0:2d:ce:c2:f0:7a:35:44:b6:bf:95:f7:96:f2:53:86:40:
        de:4e:35:41:2e:5b:6b:fa:3f:97:7d:c3:6a:cb:19:88:12:78:
        30:08:72:cc
(END)
```

What other information can you gain from the certificate:	Signature Algorithm: sha256WithRSAEncryption Issuer: Google Trust Services LLC (GTS CA 1C3) Key Usage: Digital Signature Extended Key Usage: TLS Web Server Authentication
What is the size of the public key:	Public-Key: (256 bit) *256-bit EC (elliptic curve), curve prime256v1 / NIST P-256*
Which hashing method has been used:	Signature Algorithm: sha256WithRSAEncryption *SHA-256*
Is the certificate trusted on your system:	error google.cer: verification failed *No*

A.3 `openssl s_client -connect www.live.com:443`



```
CONNECTED(00000003)
---
Certificate chain
 0 s:C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, CN=outlook.live.com
   i:C=US, O=DigiCert Inc, CN=DigiCert Cloud Services CA-1
   a:PKEY: RSA, 2048 (bit); sigalg: sha256WithRSAEncryption
   v:NotBefore: Sep 13 00:00:00 2025 GMT; NotAfter: Sep 12 23:59:59 2026 GMT
 1 s:C=US, O=DigiCert Inc, CN=DigiCert Cloud Services CA-1
   i:C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA
   a:PKEY: RSA, 2048 (bit); sigalg: sha256WithRSAEncryption
   v:NotBefore: Aug  4 12:00:00 2015 GMT; NotAfter: Aug  4 12:00:00 2030 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIHwDCCBqigAwIBAgIQDlxB7nnkWCjeMmbsu+Hj3DANBgkqhkiG9w0BAQsFADBL
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMSUwIwYDVQQDExxE
aWdpQ2VydCBDbG91ZCBTZXJ2aWNlcyBDQS0xMB4XDTI1MDkxMzAwMDAwMFoXDTI2
MDkxMjIzNTk1OVowbzELMAkGA1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24x
EDAOBgNVBAcTB1JlZG1vbmQxHjAcBgNVBAoTFU1pY3Jvc29mdCBDb3Jwb3JhdGlv
bjEZMBcGA1UEAxMQb3V0bG9vay5saXZlLmNvbTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAJs/jwFiCaO4bnPVK+bDRilRqrGeTn3MVlL0wKu5mCL5XjsT
9rEvsG0NK/iYpgKrQ4vaSBU3JO300Ggvpo1qivm8UqACYL4hAuIm7Yl3/cFcXxmb
By/nJsAqfxRTM47qQA8hMFLo0y/vns1F6BWpHOuD5cOMlHsKuS7uwLmy/ragNTRe
pucvf3nGAWdnV2rMu0SHnq5UFwJanoKsDCJxHbVDgHw0BAIeT9B/0elF2vN2TcNX
4UYgJ2dZjmw7d1Mo0kDdIEOQRQF/qUg97ILZAnv01KeIY1Wh45GoRxzusfopU1DM
Wz3EASZWUMYsKjjPDJvXI8HsixrA4tQRDFPd/F0CAwEAAaOCBHowggR2MB8GA1Ud
IwQYMBaAFN1R0KIxc6lzro+0AX5djFfLn/D3MB0GA1UdDgQWBBTs4sKie8XvJJAL
V8lNGUGYm9DTYTCCASYGA1UdEQSCAR0wggEZghBvdXRsb29rLmxpdmUuY29tghRv
dXRsb29rLXNkZi5saXZlLmNvbYIdYXR0YWNobWVudC5vdXRsb29rLm9mZmljZS5u
ZXSCIGF0dGFjaG1lbnQub3V0bG9vay5vZmZpY2VwcGUubmV0ggtob3RtYWlsLmNv
bYITKi5jYWxlbmRhci5saXZlLmNvbYINKi5ob3RtYWlsLmNvbYIKKi5saXZlLmNv
bYIPKi5tYWlsLmxpdmUuY29tghBhZmQtbC5vZmZpY2UuY29tgghsaXZlLmNvbYIW
Ki5ucmIuZm9vdHByaW50ZG5zLmNvbYIXKi5mcC5tZWFzdXJlLm9mZmljZS5jb22C
E3ByZW1pdW0ub3V0bG9vay5jb20wPgYDVR0gBDcwNTAzBgZngQwBAgIwKTAnBggr
BgEFBQcCARYbaHR0cDovL3d3dy5kaWdpY2VydC5jb20vQ1BTMA4GA1UdDwEB/wQE
AwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwgY0GA1UdHwSBhTCB
gjA/oD2gO4Y5aHR0cDovL2NybDMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0Q2xvdWRT
ZXJ2aWNlc0NBLTEtZzEuY3JsMD+gPaA7hjlodHRwOi8vY3JsNC5kaWdpY2VydC5j
b20vRGlnaUNlcnRDbG91ZFNlcnZpY2VzQ0EtMS1nMS5jcmwwfAYIKwYBBQUHAQEE
cDBuMCUGCCsGAQUFBzABhhlodHRwOi8vb2NzcHguZGlnaWNlcnQuY29tMEUGCCsG
AQUFBzAChjlodHRwOi8vY2FjZXJ0cy5kaWdpY2VydC5jb20vRGlnaUNlcnRDbG91
ZFNlcnZpY2VzQ0EtMS5jcnQwDAYDVR0TAQH/BAIwADCCAX0GCisGAQQB1nkCBAIE
ggFtBIIBaQFnAHYA1219ENGn9XfCx+lf1wC/+YLJM1pl4dCzAXMXwMjFaXcAAAGZ
QGYZsQAABAMARzBFAiEA7qFwov/ONzu2BXQStbw9Az1HZj7dBMrUW6EPCGZ+mVMC
IEiKNwciVXpNyPxt1ShRsZe7xEUKFByXoKAiqNIKgV4RAHYAwjF+V0UZo0Xufzje
spBB68fCIVoiv3/Vta12mtkOUs0AAAGZQGYZ8gAABAMARzBFAiEA4n5GL8g+cSoT
+QhHWl7CeQfH5GqB7RfAzv9o1rIvhBoCIHikhkpi/kkZfVrGQRlm2rJ1wuJKKYM6
xJBHL/S5e9FoAHUAlE5Dh/rswe+B8xkkJqgYZQHH0184AgE/cmd9VTcuGdgAAAGZ
QGYaBAAABAMARjBEAiBZPd1uIswhQN7wZISWB44CAkac96k8x+6Pnd9PgMGogAIg
:
```



```
subject=C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, CN=outlook.live.com
issuer=C=US, O=DigiCert Inc, CN=DigiCert Cloud Services CA-1
---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: rsa_pss_rsae_sha256
Peer Temp Key: ECDH, secp521r1, 521 bits
---
SSL handshake has read 3851 bytes and written 2323 bytes
Verification: OK
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Protocol: TLSv1.3
Server public key is 2048 bit
This TLS version forbids renegotiation.
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
---
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID: 717FD491E2ED8E390CFFDC0557DDAC628786676355AF6CFEF3566EA531A4CA7B
    Session-ID-ctx:
    Resumption PSK: 089676B07B702461FBA20EDB9D169712CA3C9CAE88AD70C7910A3DB23BA44A388B304C272314DC299CB989BD5E75F10D
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 36000 (seconds)
    TLS session ticket:
    0000 - 00 00 00 00 2c 9a 5b b1-74 66 99 46 ab ca 21 cb   ....,.[.tf.F..!.
    0010 - 55 96 44 27 53 e5 40 c1-5a 4f f0 c2 31 6a 7c 91   U.D'S.@.ZO..1j|.
    0020 - fa 68 cf 80 06 66 e9 a7-6f be bb 21 51 a8 10 d8   .h...f..o..!Q...
    0030 - b6 b6 cc 49 5f ba 5f 7b-53 c4 69 20 02 4f 7d 93   ...I_._{S.i .O}.
    0040 - 80 b7 78 40 16 e4 d2 b6-93 a1 4a 88 7d c0 df 56   ..x@......J.}..V
    0050 - 8a 89 9a f1 0c 17 43 02-1a 21 ca f3 90 3e 55 3a   ......C..!...>U:
    0060 - ed bf c1 4f 56 b8 39 12-06 32 36 4f 85 f2 b4 4e   ...OV.9..26O...N
    0070 - de 4b 10 15 81 7a 83 89-e7 11 59 fe 7a 06 3f fb   .K...z....Y.z.?.
    0080 - a8 9f 53 d7 97 67 d0 79-57 46 3f be 54 37 0d 19   ..S..g.yWF?.T7..
    0090 - b2 29 27 ca e6 18 f0 42-48 dd 60 6d ec b5 b5 0c   .)'....BH.`m....
    00a0 - 3b 4e e7 ee 46 fe 6f 60-b3 76 24 21 b8 a5 41 1c   ;N..F.o`.v$!..A.
    00b0 - 3b 0f 2c 5c ea b8 33 6d-b3 35 cd 51 a0 21 ff 89   ;.,\..3m.5.Q.!..
    00c0 - a7 d0 78 fa 78 9c 84 4a-e5 4a 65 48 61 1c 09 3a   ..x.x..J.JeHa..:
    00d0 - 61 43 04 3e 90 e3 c0 cc-54 6a af 2c f5 8e 0d 43   aC.>....Tj.,...C
    00e0 - 0a ed 5f 02 04 7c f7 21-ee e4 30 29 cd 4d 3c 20   .._..|.!..0).M<
:
```

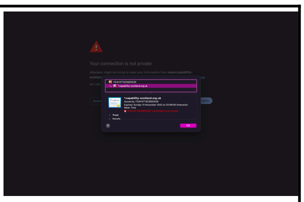
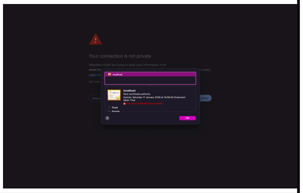
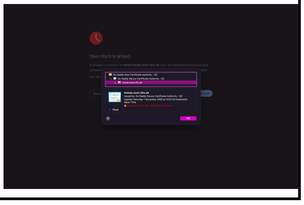
Certificate Chain (from leaf → root):

1. Leaf certificate (server certificate)
    - CN = outlook.live.com
    - O = Microsoft Corporation
    - Issued by DigiCert Cloud Services CA-1
2. Intermediate CA
    - CN = DigiCert Cloud Services CA-1
    - Issued by DigiCert Global Root CA
3. Root CA
    - CN = DigiCert Global Root CA
    - Self-signed (trusted root)

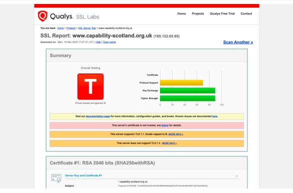
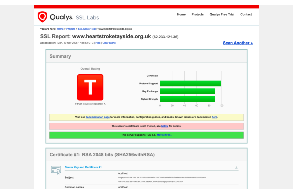
Subject(Leaf Certificate):
subject=C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, CN=outlook.live.com

Issuer(Leaf Certificate):
issuer=C=US, O=DigiCert Inc, CN=DigiCert Cloud Services CA-1

A.4 A scan, at the time, on health and social care sites from the following page showed problems in digital certificates:
https://bit.ly/2EkUvX0

https://www.capability-scotland.org.uk	Expired: Sunday 13 November 2022 at 23:59:59	 Your connection is not private Attackers might be trying to steal your information from www.capability-scotland.org.uk FG4H1FT923900529 *.capability-scotland.org.uk *.capability-scotland.org.uk Issued by: FG4H1FT923900529 Expired: Sunday 13 November 2022 at 23:59:59 Greenwich Mean Time "FG4H1FT923900529" certificate is not trusted Trust Details OK
https://www.heartstroketayside.org.uk	localhost (is not trusted) Root certificate authority	 Your connection is not private Attackers might be trying to steal your information from localhost localhost Root certificate authority Expires: Saturday 17 January 2026 at 15:58:45 Greenwich Mean Time This root certificate is not trusted Trust Details OK
https://www.travax.scot.nhs.uk	Expired: Saturday 1 November 2025 at 14:57:22	 Your clock is ahead A private connection to www.travax.scot.nhs.uk can't be established because your Go Daddy Root Certificate Authority - G2 Go Daddy Secure Certificate Authority - G2 travax.scot.nhs.uk travax.scot.nhs.uk Issued by: Go Daddy Secure Certificate Authority - G2 Expired: Saturday 1 November 2025 at 14:57:22 Greenwich Mean Time "travax.scot.nhs.uk" certificate is expired Trust OK

www.ssllabs.com

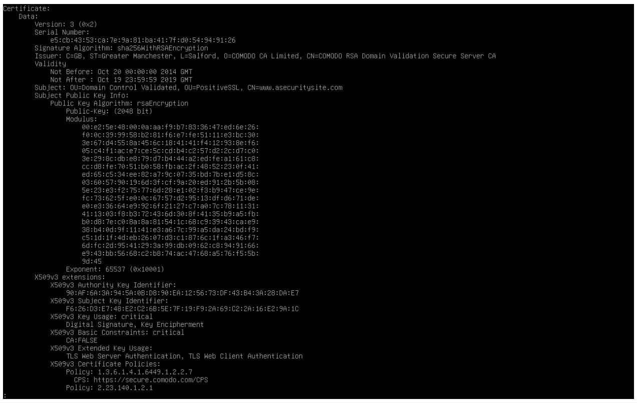
https://www.capability-scotland.org.uk ssllabs this website	Sun, 13 Nov 2022 23:59:59 UTC (expired 2 years and 11 months ago) EXPIRED	 Qualys. SSL Labs Home Projects Qualys Free Trial Contact You are here: Home > Projects > SSL Server Test > www.capability-scotland.org.uk SSL Report: www.capability-scotland.org.uk (185.122.65.65) Assessed on: Mon, 10 Nov 2025 17:27:31 UTC | Hide | Clear cache Scan Another » Summary Overall Rating T If trust issues are ignored: B Certificate Protocol Support Key Exchange Cipher Strength 0 20 40 60 80 100 Visit our documentation page for more information, configuration guides, and books. Known issues are documented here. This server's certificate is not trusted, see below for details. This server supports TLS 1.1. Grade capped to B. MORE INFO » This server does not support TLS 1.3. MORE INFO » Certificate #1: RSA 2048 bits (SHA256withRSA) Server Key and Certificate #1 Subject *.capability-scotland.org.uk **T Rating**
https://www.heartstroketayside.org.uk	Alternative names - INVALID	 Qualys. SSL Labs Home Projects Qualys Free Trial Contact You are here: Home > Projects > SSL Server Test > www.heartstroketayside.org.uk SSL Report: www.heartstroketayside.org.uk (62.233.121.36) Assessed on: Mon, 10 Nov 2025 17:35:52 UTC | Hide | Clear cache Scan Another » Summary Overall Rating T If trust issues are ignored: A Certificate Protocol Support Key Exchange Cipher Strength 0 20 40 60 80 100 Visit our documentation page for more information, configuration guides, and books. Known issues are documented here. This server's certificate is not trusted, see below for details. This server supports TLS 1.3. MORE INFO » Certificate #1: RSA 2048 bits (SHA256withRSA) Server Key and Certificate #1 Subject localhost Common names localhost **T Rating**

A.5 Example 2 to Example 6

Cert	Organisation (Issued to)	Date range when valid	Size of public key	Issuer	Root CA	Hash method	Is it trusted?
2	No One / Nowhere Ltd (CN=No One)	Oct 29 2011 – Oct 28 2013	1024-bit RSA	No One (self-signed)	None (self-signed)	sha1WithRSAEncryption	No
3	Google (CN=*.google.com)	Feb 08 2023 – May 03 2023	256-bit EC (P-256)	GTS CA 1C3	Google Trust Services Root	sha256WithRSAEncryption	No
4	Cisco Systems (CN=www.cisco.com)	Jul 10 2012 – Jul 11 2013	1024-bit RSA	VeriSign Class 3 Secure Server CA - G3	VeriSign Root	sha1WithRSAEncryption	No
5	Microsoft Corporation (CN=microsoft.com)	Jan 13 2023 – Jan 08 2024	2048-bit RSA	Microsoft Azure TLS Issuing CA 05	Microsoft Root CA	sha384WithRSAEncryption	No
6	Oracle Corporation (CN=oracle.com)	Feb 14 2023 – Feb 26 2024	2048-bit RSA	DigiCert TLS RSA SHA256 2020 CA1	DigiCert Root	sha256WithRSAEncryption	No

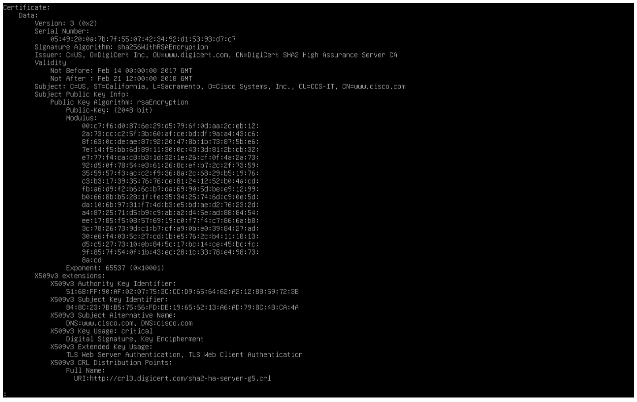
A.6 `openssl x509 -inform der -in [certname] -noout -text`

http://asecuritysite.com/der.zip

asecuritysite.der	

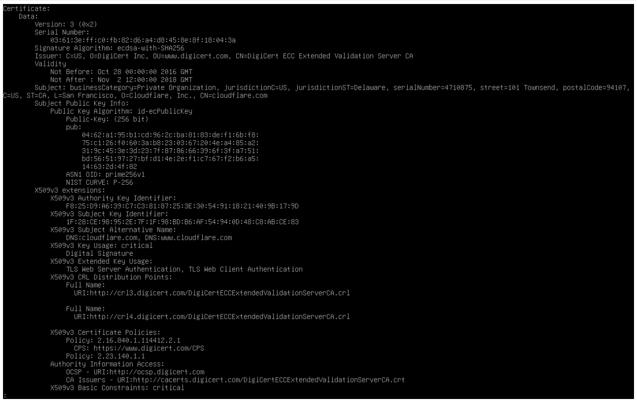
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            e5:cb:43:53:ca:7e:9a:81:ba:41:7f:d0:54:94:91:26
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Domain Validation Secure Server CA
        Validity
            Not Before: Oct 20 00:00:00 2014 GMT
            Not After : Oct 19 23:59:59 2019 GMT
        Subject: OU=Domain Control Validated, OU=PositiveSSL, CN=www.asecuritysite.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:e2:5e:48:00:0a:aa:f9:b7:83:36:47:ed:6e:26:
                    f0:0c:39:99:58:b2:81:f6:e7:fe:51:11:e3:bc:30:
                    3e:67:d4:55:8a:45:6c:18:41:41:f4:12:93:8e:f6:
                    05:c4:f1:ac:e7:ce:5c:cd:b4:c2:57:d2:2c:d7:c0:
                    3e:29:8c:db:e8:79:d7:b4:44:a2:ed:fe:a1:61:c8:
                    cc:d8:fe:70:51:b0:58:fb:ac:2f:48:52:23:0f:41:
                    ed:65:c5:34:ee:82:a7:9c:07:35:bd:7b:e1:d5:8c:
                    03:60:57:90:19:6d:3f:cf:9a:20:ed:91:2b:5b:08:
                    5e:23:e3:f2:75:77:6d:28:e1:02:f3:b9:47:ce:9e:
                    fc:73:62:5f:e0:0c:67:57:d2:95:13:df:d6:71:de:
                    e0:e3:36:64:e9:92:6f:21:27:c7:a0:7c:78:11:31:
                    41:13:03:f8:b3:72:43:6d:30:8f:41:35:b9:a5:fb:
                    b0:d8:7e:c0:8a:8a:81:54:1c:68:c9:39:43:ca:e9:
                    38:b4:0d:9f:11:41:e3:a6:7c:99:a5:da:24:bd:f9:
                    c5:1d:1f:4d:eb:26:07:d3:c1:87:6c:1f:a3:46:f7:
                    6d:fc:2d:95:41:29:3a:99:db:09:62:c8:94:91:66:
                    e9:43:bb:56:68:c2:b8:74:ac:47:68:a5:76:f5:5b:
                    9d:45
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                90:AF:6A:3A:94:5A:0B:D8:90:EA:12:56:73:DF:43:B4:3A:28:DA:E7
            X509v3 Subject Key Identifier:
                F6:26:D3:E7:48:E2:C2:6B:5E:7F:19:F9:2A:69:C2:2A:16:E2:9A:1C
            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: 1.3.6.1.4.1.6449.1.2.2.7
                  CPS: https://secure.comodo.com/CPS
                Policy: 2.23.140.1.2.1
:
```

cisco.der



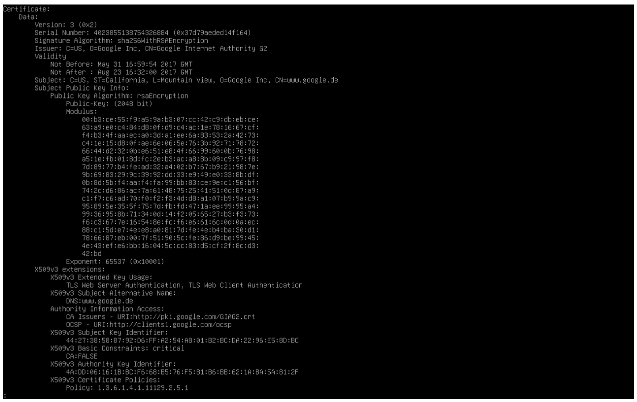
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            05:49:20:0a:7b:7f:55:07:42:34:92:d1:53:93:d7:c7
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
        Validity
            Not Before: Feb 14 00:00:00 2017 GMT
            Not After : Feb 21 12:00:00 2018 GMT
        Subject: C=US, ST=California, L=Sacramento, O=Cisco Systems, Inc., OU=CCS-IT, CN=www.cisco.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c7:f6:d0:87:6e:29:d5:79:6f:0d:aa:2c:eb:12:
                    2a:73:cc:c2:5f:3b:60:af:ce:bd:df:9a:a4:43:c6:
                    8f:63:0c:de:ae:87:92:20:47:8b:1b:73:87:5b:e6:
                    7e:14:f5:bb:6d:89:11:30:0c:43:3d:81:2b:cb:32:
                    e7:77:f4:ca:c8:b3:1d:32:1e:26:cf:0f:4a:2a:73:
                    92:d5:0f:78:54:e3:61:26:8c:ef:b7:2c:2f:73:59:
                    35:59:57:f3:ac:c2:f9:36:8a:2c:68:29:b5:19:76:
                    c3:b3:17:39:35:76:76:ce:81:24:12:52:b0:4a:cd:
                    fb:a6:d9:f2:b6:6c:b7:da:69:90:5d:be:e9:12:99:
                    b0:66:8b:b5:28:1f:fe:35:34:25:74:6d:c9:0e:5d:
                    da:10:6b:97:31:f7:4d:b3:e5:bd:ae:d2:76:23:2d:
                    a4:87:25:71:d5:b9:c9:ab:a2:d4:5e:ad:88:84:54:
                    ee:17:85:f5:08:57:69:19:c0:f7:f4:c7:86:6a:b8:
                    3c:78:26:73:9d:c1:b7:cf:a9:0b:e0:39:84:27:ad:
                    30:e6:f4:03:5c:27:cd:1b:e5:76:2c:b4:11:18:13:
                    d5:c5:27:73:10:eb:84:5c:17:bc:14:ce:45:bc:fc:
                    9f:85:7f:54:0f:1b:43:ec:28:1c:33:78:e4:98:73:
                    8a:cd
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                51:68:FF:90:AF:02:07:75:3C:CC:D9:65:64:62:A2:12:B8:59:72:3B
            X509v3 Subject Key Identifier:
                84:8C:23:7B:B5:75:56:FD:DE:19:65:62:13:A6:AD:79:8C:4B:CA:4A
            X509v3 Subject Alternative Name:
                DNS:www.cisco.com, DNS:cisco.com
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl3.digicert.com/sha2-ha-server-g5.crl

:
```

cloudflare.der



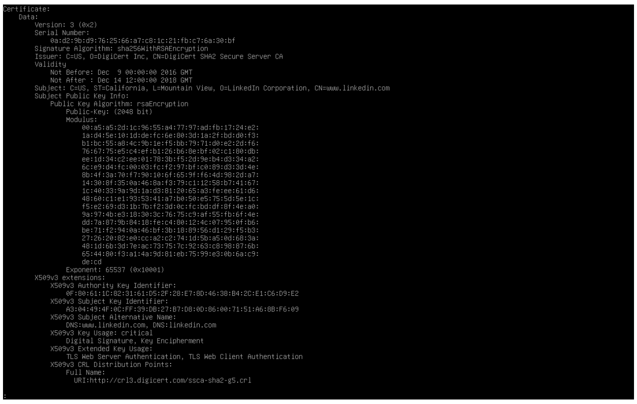
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:61:3e:ff:c0:fb:82:d6:a4:d8:45:8e:8f:18:04:3a
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert ECC Extended Validation Server CA
        Validity
            Not Before: Oct 28 00:00:00 2016 GMT
            Not After : Nov  2 12:00:00 2018 GMT
        Subject: businessCategory=Private Organization, jurisdictionC=US, jurisdictionST=Delaware, serialNumber=4710875, street=101 Townsend, postalCode=94107,
C=US, ST=CA, L=San Francisco, O=Cloudflare, Inc., CN=cloudflare.com
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:62:a1:95:b1:cd:96:2c:ba:81:83:de:f1:6b:f8:
                    75:c1:26:f0:60:3a:b8:23:03:67:20:4e:a4:85:a2:
                    31:9c:45:3e:3d:23:7f:87:86:66:39:6f:3f:a7:51:
                    bd:56:51:97:27:bf:d1:4e:2e:f1:c7:67:f2:b6:a5:
                    14:63:2d:4f:82
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                F8:25:D9:A6:39:C7:C3:81:87:25:3E:30:54:91:18:21:40:9B:17:9D
            X509v3 Subject Key Identifier:
                1F:28:CE:98:95:2E:7F:1F:98:BD:B6:AF:54:94:0D:48:C8:AB:CE:83
            X509v3 Subject Alternative Name:
                DNS:cloudflare.com, DNS:www.cloudflare.com
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl3.digicert.com/DigiCertECCExtendedValidationServerCA.crl

                Full Name:
                  URI:http://crl4.digicert.com/DigiCertECCExtendedValidationServerCA.crl

            X509v3 Certificate Policies:
                Policy: 2.16.840.1.114412.2.1
                  CPS: https://www.digicert.com/CPS
                Policy: 2.23.140.1.1
            Authority Information Access:
                OCSP - URI:http://ocsp.digicert.com
                CA Issuers - URI:http://cacerts.digicert.com/DigiCertECCExtendedValidationServerCA.crt
            X509v3 Basic Constraints: critical
:
```

google.der



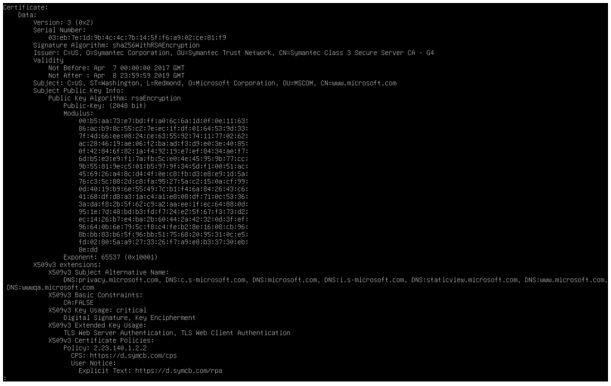
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4023855138754326884 (0x37d79aeded14f164)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Google Inc, CN=Google Internet Authority G2
        Validity
            Not Before: May 31 16:59:54 2017 GMT
            Not After : Aug 23 16:32:00 2017 GMT
        Subject: C=US, ST=California, L=Mountain View, O=Google Inc, CN=www.google.de
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b3:ce:55:f9:a5:9a:b3:07:cc:42:c9:db:eb:ce:
                    63:a9:e0:c4:84:d8:0f:d9:c4:ac:1e:78:16:67:cf:
                    f4:b3:4f:aa:ec:a0:3d:a1:ee:6a:83:53:2a:42:73:
                    c4:1e:15:d8:0f:ae:6e:06:5e:76:3b:92:71:78:72:
                    66:44:d2:32:0b:e6:51:e8:4f:66:99:60:0b:76:98:
                    a5:1e:fb:01:8d:fc:2e:b3:ac:a8:8b:09:c9:97:f8:
                    7d:89:77:b4:fe:ad:32:a4:02:b7:67:b9:21:98:7e:
                    9b:69:83:29:9c:39:92:dd:33:e9:49:e0:33:8b:df:
                    0b:8d:5b:f4:aa:f4:fa:99:bb:83:ce:9e:c1:56:bf:
                    74:2c:d6:86:ac:7a:61:48:75:25:41:51:0d:87:a9:
                    c1:f7:c6:ad:70:f0:f2:f3:4d:d8:a1:07:b9:9a:c9:
                    95:89:5e:35:5f:75:7d:fb:fd:47:1a:ee:99:95:a4:
                    99:36:95:8b:71:34:0d:14:f2:05:65:27:b3:f3:73:
                    f6:c3:67:7e:16:54:8e:fc:f6:e6:61:6c:0d:0a:ec:
                    88:c1:5d:e7:4e:e8:a0:81:7d:fe:4e:b4:ba:30:d1:
                    78:66:87:eb:00:7f:51:90:5c:fe:86:d9:be:99:45:
                    4e:43:ef:e6:bb:16:04:5c:cc:83:d5:cf:2f:8c:d3:
                    42:bd
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Subject Alternative Name:
                DNS:www.google.de
            Authority Information Access:
                CA Issuers - URI:http://pki.google.com/GIAG2.crt
                OCSP - URI:http://clients1.google.com/ocsp
            X509v3 Subject Key Identifier:
                44:27:38:58:87:92:D6:FF:A2:54:A8:01:B2:BC:DA:22:96:E5:8D:BC
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Authority Key Identifier:
                4A:DD:06:16:1B:BC:F6:68:B5:76:F5:81:B6:BB:62:1A:BA:5A:81:2F
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.11129.2.5.1
:
```

linkedin.der



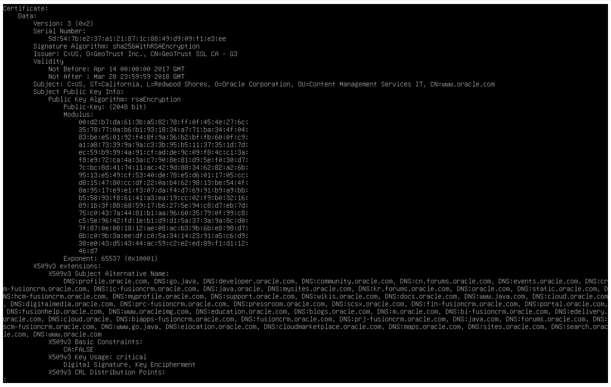
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0a:d2:9b:d9:76:25:66:a7:c8:1c:21:fb:c7:6a:30:bf
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
        Validity
            Not Before: Dec  9 00:00:00 2016 GMT
            Not After : Dec 14 12:00:00 2018 GMT
        Subject: C=US, ST=California, L=Mountain View, O=LinkedIn Corporation, CN=www.linkedin.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a5:a5:2d:1c:96:55:a4:77:97:ad:fb:17:24:e2:
                    1a:d4:5e:10:1d:de:fc:6e:80:3d:1a:2f:bd:d0:f3:
                    b1:bc:55:a8:4c:9b:1e:f5:bb:79:71:d0:e2:2d:f6:
                    76:67:75:e5:c4:ef:b1:26:b6:8e:bf:02:c1:80:db:
                    ee:1d:34:c2:ee:01:78:3b:f5:2d:9e:b4:d3:34:a2:
                    6c:e9:d4:fc:00:03:fc:f2:97:bf:c0:89:d3:3d:4e:
                    8b:4f:3a:70:f7:90:10:6f:65:9f:f6:4d:98:2d:a7:
                    14:30:8f:35:0a:46:8a:f3:79:c1:12:58:b7:41:67:
                    1c:40:33:9a:9d:1a:d3:81:20:65:a3:fe:ee:61:d6:
                    48:60:c1:e1:93:53:41:a7:b0:50:e5:75:5d:5e:1c:
                    f5:e2:69:d3:1b:7b:f2:3d:0c:fc:bd:df:8f:4e:a0:
                    9a:97:4b:e3:18:30:3c:76:75:c9:af:55:fb:6f:4e:
                    dd:7a:87:9b:84:18:fe:c4:80:12:4c:07:95:0f:b6:
                    be:71:f2:94:0a:46:bf:3b:18:89:56:d1:29:f5:b3:
                    27:26:20:82:e0:cc:a2:c2:74:1d:5b:a5:0d:68:3a:
                    48:1d:6b:3d:7e:ac:73:75:7c:92:63:c8:98:87:6b:
                    65:44:80:f3:a1:4a:9d:81:eb:75:99:e3:0b:6a:c9:
                    de:cd
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                0F:80:61:1C:82:31:61:D5:2F:28:E7:8D:46:38:B4:2C:E1:C6:D9:E2
            X509v3 Subject Key Identifier:
                A3:04:49:4F:0C:FF:39:DB:27:B7:D8:0D:86:00:71:51:A6:8B:F6:09
            X509v3 Subject Alternative Name:
                DNS:www.linkedin.com, DNS:linkedin.com
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl3.digicert.com/ssca-sha2-g5.crl

:
```

microsoft.der



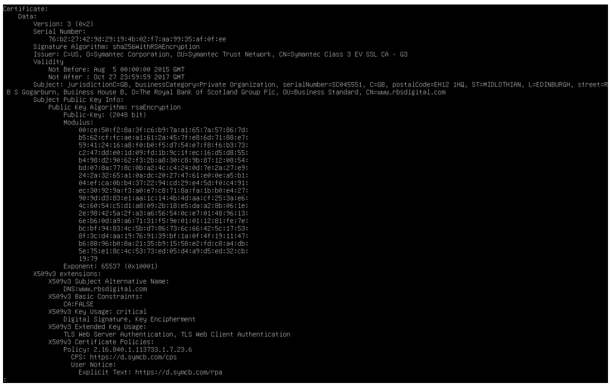
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:eb:7e:1d:9b:4c:4c:7b:14:5f:f6:a9:02:ce:81:f9
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4
        Validity
            Not Before: Apr  7 00:00:00 2017 GMT
            Not After : Apr  8 23:59:59 2019 GMT
        Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, OU=MSCOM, CN=www.microsoft.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b5:aa:73:e7:bd:ff:a0:6c:6a:1d:0f:0e:11:63:
                    86:ac:b9:8c:55:c2:7e:ec:1f:df:01:64:53:9d:33:
                    7f:4d:66:ee:08:24:ce:63:55:92:74:11:77:02:62:
                    ac:28:46:19:ae:06:f2:ba:ad:f3:d9:e0:3e:40:85:
                    0f:42:84:6f:82:1a:f4:92:19:e7:ef:84:34:ae:f7:
                    6d:b5:e3:e9:f1:7a:fb:5c:e0:4e:45:95:9b:77:cc:
                    9b:55:81:9e:c5:01:b5:97:9f:34:5d:f1:00:51:ac:
                    45:69:26:a4:8c:d4:4f:0e:c8:fb:d3:e8:e9:1d:5a:
                    76:c3:5c:88:2d:c8:fa:95:27:5a:c2:15:0a:cf:99:
                    0d:40:19:b9:6e:55:49:7c:b1:f4:6a:84:26:43:c6:
                    41:68:df:d8:a3:1a:c4:a1:e8:08:df:71:0c:53:36:
                    3a:da:f8:2b:5f:62:c9:a2:aa:ee:1f:ec:64:88:0d:
                    95:1e:7d:48:bd:b3:fd:f7:24:e2:5f:67:f3:73:d2:
                    ec:14:26:b7:e4:ba:2b:60:44:2a:42:32:0d:3f:ef:
                    96:64:0b:6e:79:5c:f8:c4:fe:b2:8e:16:08:cb:96:
                    8b:bb:83:b6:5f:96:bb:51:75:68:20:95:31:0c:e5:
                    fd:02:80:5a:a9:27:33:26:f7:a9:e8:b3:37:30:eb:
                    8e:dd
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:privacy.microsoft.com, DNS:c.s-microsoft.com, DNS:microsoft.com, DNS:i.s-microsoft.com, DNS:staticview.microsoft.com, DNS:www.microsoft.com,
 DNS:wwwqa.microsoft.com
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.2
                  CPS: https://d.symcb.com/cps
                  User Notice:
                    Explicit Text: https://d.symcb.com/rpa
:
```

oracle.der



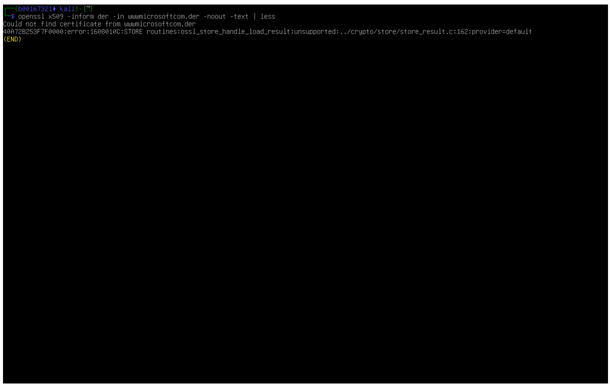
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            5d:54:7b:e2:37:a1:21:87:1c:88:49:d9:09:f1:e3:ee
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3
        Validity
            Not Before: Apr 14 00:00:00 2017 GMT
            Not After : Mar 28 23:59:59 2018 GMT
        Subject: C=US, ST=California, L=Redwood Shores, O=Oracle Corporation, OU=Content Management Services IT, CN=www.oracle.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d2:b7:da:61:3b:a5:82:78:ff:0f:45:4e:27:6c:
                    35:78:77:0a:b6:b1:93:18:34:a7:71:ba:34:4f:04:
                    83:be:e5:01:92:f4:8f:9a:36:b2:bf:fb:60:0f:c9:
                    a1:a8:73:39:9a:9a:c3:3b:95:b5:11:37:35:1d:7d:
                    ec:59:b9:99:4a:91:cf:ad:de:9c:09:f8:4c:c1:3a:
                    f8:e9:72:ca:4a:3a:c7:90:8e:81:d9:5e:f0:30:d7:
                    7c:bc:8d:41:74:11:ac:42:9d:88:34:62:82:a2:6b:
                    95:13:e5:49:cf:53:40:de:78:e5:d6:01:17:05:cc:
                    d8:15:47:80:cc:df:22:0a:b4:62:98:13:be:54:4f:
                    8a:95:17:e9:e1:f3:07:da:f4:d7:69:91:b9:a9:bb:
                    b5:58:93:f8:61:41:a3:ea:19:cc:02:f9:b0:32:16:
                    89:1b:3f:88:68:59:17:b6:27:5e:94:c8:d7:eb:7d:
                    75:c0:43:7a:44:81:b1:aa:96:60:35:79:0f:99:c8:
                    c5:5e:96:42:fd:1e:b1:d9:d1:5a:37:3a:9a:8c:d0:
                    7f:87:0e:08:18:12:ae:08:ac:b3:9b:6b:e8:98:d7:
                    8b:c0:9b:3a:ee:df:c0:5a:34:14:23:91:a5:c6:d9:
                    38:e0:43:d5:43:44:ac:59:c2:e2:ed:89:f1:d1:12:
                    46:d7
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:profile.oracle.com, DNS:go.java, DNS:developer.oracle.com, DNS:community.oracle.com, DNS:cn.forums.oracle.com, DNS:events.oracle.com, DNS:cr
m-fusioncrm.oracle.com, DNS:ic-fusioncrm.oracle.com, DNS:java.oracle, DNS:mysites.oracle.com, DNS:kr.forums.oracle.com, DNS:oracle.com, DNS:static.oracle.com, D
NS:hcm-fusioncrm.oracle.com, DNS:myprofile.oracle.com, DNS:support.oracle.com, DNS:wikis.oracle.com, DNS:docs.oracle.com, DNS:www.java.com, DNS:cloud.oracle.com
, DNS:digitalmedia.oracle.com, DNS:prc-fusioncrm.oracle.com, DNS:pressroom.oracle.com, DNS:scsx.oracle.com, DNS:fin-fusioncrm.oracle.com, DNS:portal.oracle.com,
 DNS:fusionhelp.oracle.com, DNS:www.oracleimg.com, DNS:education.oracle.com, DNS:blogs.oracle.com, DNS:m.oracle.com, DNS:bi-fusioncrm.oracle.com, DNS:edelivery.
oracle.com, DNS:cloud.oracle, DNS:biapps-fusioncrm.oracle.com, DNS:fusioncrm.oracle.com, DNS:prj-fusioncrm.oracle.com, DNS:java.com, DNS:forums.oracle.com, DNS:
scm-fusioncrm.oracle.com, DNS:www.go.java, DNS:elocation.oracle.com, DNS:cloudmarketplace.oracle.com, DNS:maps.oracle.com, DNS:sites.oracle.com, DNS:search.orac
le.com, DNS:www.oracle.com
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 CRL Distribution Points:
:
```

rbs.der



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            76:b2:27:42:9d:29:19:4b:02:f7:aa:99:35:af:0f:ee
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL CA - G3
        Validity
            Not Before: Aug  5 00:00:00 2015 GMT
            Not After : Oct 27 23:59:59 2017 GMT
        Subject: jurisdictionC=GB, businessCategory=Private Organization, serialNumber=SC045551, C=GB, postalCode=EH12 1HQ, ST=MIDLOTHIAN, L=EDINBURGH, street=R
 B S Gogarburn, Business House B, O=The Royal Bank of Scotland Group Plc, OU=Business Standard, CN=www.rbsdigital.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ce:50:f2:8a:3f:c6:b9:7a:a1:65:7a:57:86:7d:
                    b5:62:cf:fc:ae:a1:61:2a:45:7f:e8:6d:71:88:e7:
                    59:41:24:16:a8:f0:b0:f5:d7:54:e7:f8:f6:b3:73:
                    c2:47:dd:e0:1d:09:fd:1b:9c:1f:ec:16:d5:d8:55:
                    b4:98:d2:90:62:f3:2b:a8:30:c8:9b:87:12:08:54:
                    bd:07:8a:77:8c:0b:a2:4c:c4:24:0d:7e:2a:27:e9:
                    24:2a:32:65:a1:0a:dc:20:27:47:61:e0:0e:a5:b1:
                    04:ef:ca:0b:b4:37:22:94:cd:29:e4:5d:f0:c4:91:
                    ec:30:92:9a:f3:a0:e7:c8:71:8a:fa:1b:b0:e4:27:
                    90:9d:d3:83:e1:aa:1c:14:4b:4d:aa:cf:25:3a:e6:
                    4c:60:54:c5:d1:a8:09:2b:18:e5:da:a2:8b:06:1e:
                    2e:98:42:5a:2f:a3:a6:56:54:0c:e7:01:48:96:13:
                    6e:b6:0d:a9:a6:71:31:f5:9e:01:01:12:81:fe:7e:
                    bc:bf:94:83:4c:5b:d7:86:73:6c:66:42:5c:17:53:
                    8f:3c:d4:aa:19:76:91:39:bf:1a:0f:4f:19:11:47:
                    b6:88:96:b0:8a:21:35:b9:15:58:e2:fd:c8:a4:db:
                    5e:75:e1:8c:4c:53:73:ed:05:d4:a9:d5:ed:32:cb:
                    19:79
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:www.rbsdigital.com
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Certificate Policies:
                Policy: 2.16.840.1.113733.1.7.23.6
                  CPS: https://d.symcb.com/cps
                  User Notice:
                    Explicit Text: https://d.symcb.com/rpa
:
```

wwwmicrosoftcom.der



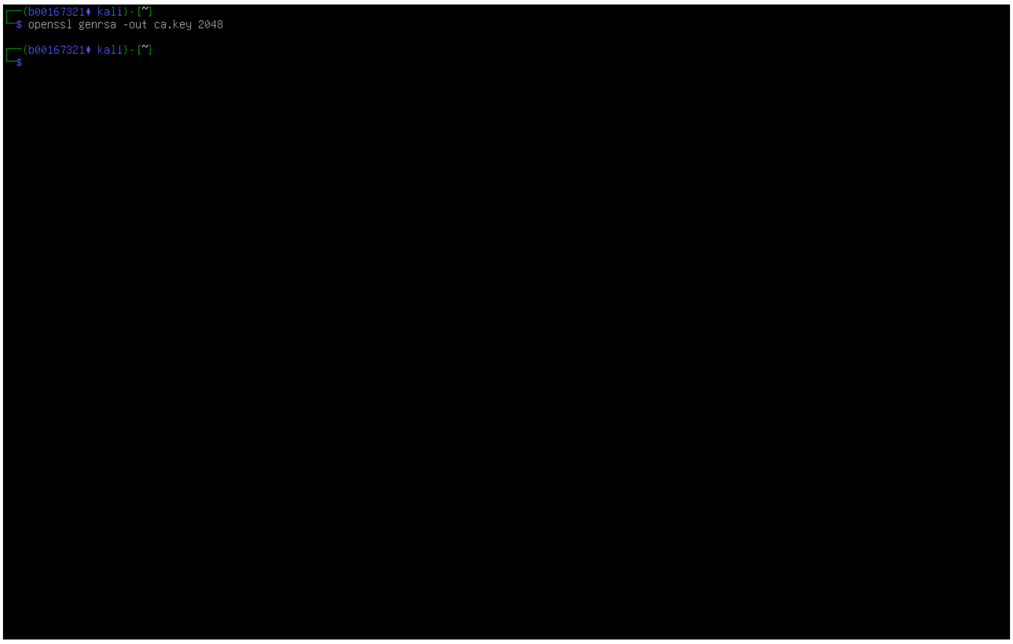
```
┌──(b00167321♦ kali)-[~]
└─$ openssl x509 -inform der -in wwwmicrosoftcom.der -noout -text | less
Could not find certificate from wwwmicrosoftcom.der
40A72B253F7F0000:error:1608010C:STORE routines:ossl_store_handle_load_result:unsupported:../crypto/store/store_result.c:162:provider=default
(END)
```

B. Creating certificates

B.1 `openssl genrsa -out ca.key 2048`

Create a Private Key for CA using OpenSSL

- `genrsa` → generates an RSA private key
- `-out ca.key` → saves the key to a file named ca.key
- `2048` → key length in bits (can be 4096 for higher security)



```
┌──(b00167321♦ kali)-[~]
└─$ openssl genrsa -out ca.key 2048

┌──(b00167321♦ kali)-[~]
└─$
```

→ **A 2048-bit RSA private key stored in ca.key**

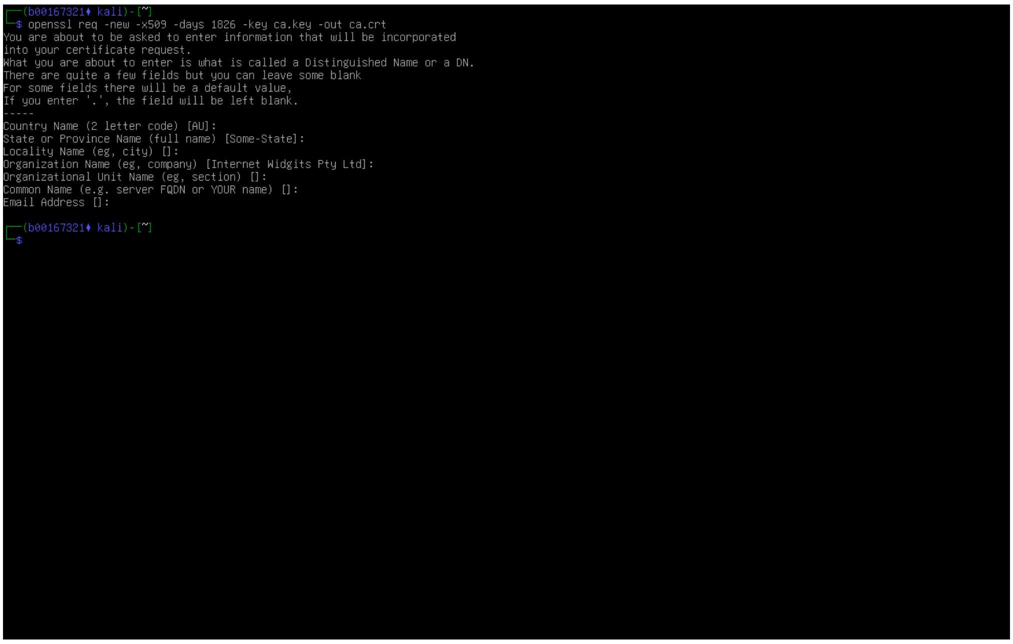
→ **This key will be used to sign other certificates** (it is the Root CA's private key)

This command generates a new RSA private key for the Certificate Authority (CA). `genrsa` creates an unencrypted key, and `-out ca.key` saves it as a file

B.2 `openssl req -new -x509 -days 1826 -key ca.key -out ca.crt`

Generate the certificate using OpenSSL

- `req` → create a certificate request
- `-new -x509` → generate a self-signed X.509 certificate
- `-days 1826` → certificate validity (5 years)
- `-key ca.key` → use the private key created earlier
- `-out ca.crt` → output file (the new CA certificate)



```
┌──(b00167321♦ kali)-[~]
└─$ openssl req -new -x509 -days 1826 -key ca.key -out ca.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

┌──(b00167321♦ kali)-[~]
└─$
```

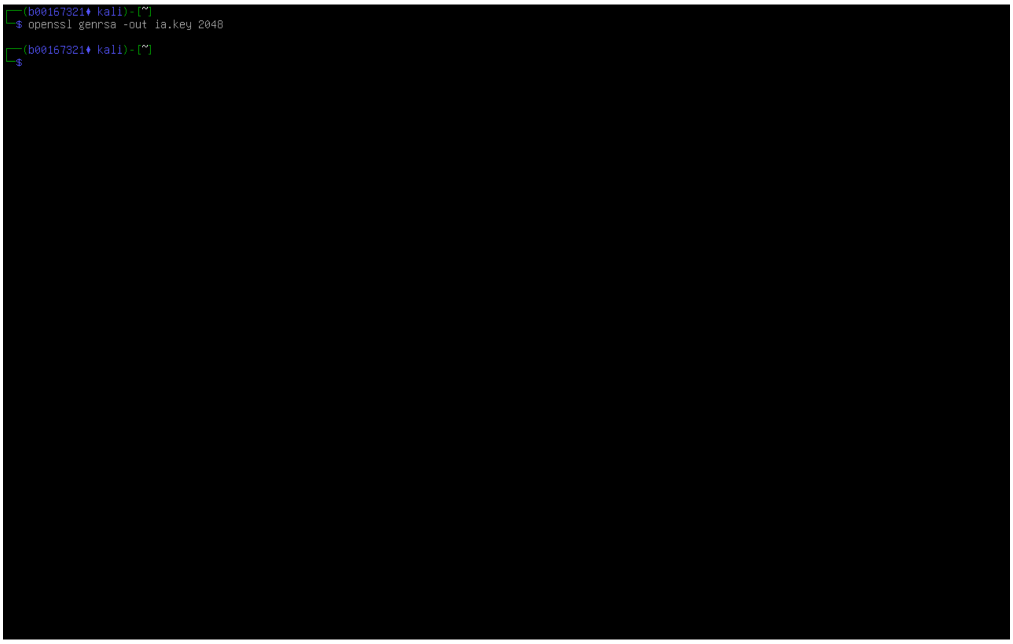
→ **Generated a self-signed CA certificate valid for 1826 days**
→ **Output file: ca.crt**
→ **This certificate includes the public key + issuer information**

This creates the Root Certificate.
Because no external CA signs it, `-x509` makes it self-signed, meaning it signs itself using `ca.key`.

B.3 `openssl genrsa -out ia.key 2048`

Generate a private key using OpenSSL

- `genrsa` → generates an RSA private key
- `-out ia.key` → saves the key to a file named ia.key
- `2048` → key length in bits (can be 4096 for higher security)



```
┌──(b00167321♦ kali)-[~]
└─$ openssl genrsa -out ia.key 2048

┌──(b00167321♦ kali)-[~]
└─$
```

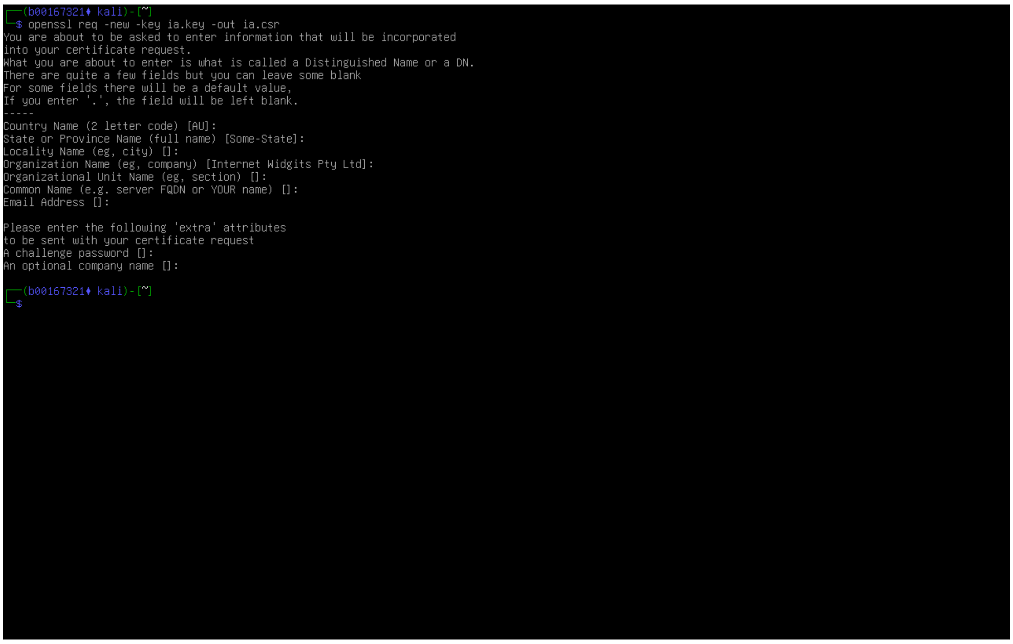
→ **Created a 2048-bit RSA private key for the intermediate authority**
→ **File ia.key will be used to create a CSR next**

This is the private key for the subordinate CA, also called “Intermediate CA.”

B.4 `openssl req -new -key ia.key -out ia.csr`

We now create a Certificate Signing Request (CSR) — a file containing identity details and the public key.

- `req -new` → creates a new certificate request
- `-key ia.key` → uses the subordinate CA’s private key
- `-out ia.csr` → saves the request in ia.csr



```
┌──(b00167321♦ kali)-[~]
└─$ openssl req -new -key ia.key -out ia.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

┌──(b00167321♦ kali)-[~]
└─$
```

→ **Output file: ia.csr**

→ **Contains:**

- **Intermediate CA’s public key**
- **Identity information**
- **Intended certificate fields**

A CSR is like an "application form" sent to a CA to request a certificate.
It contains the public key and subject (organisation) information, but not a signature yet.

B.5 `cat ia.csr` `openssl req -in ia.csr -noout -text`

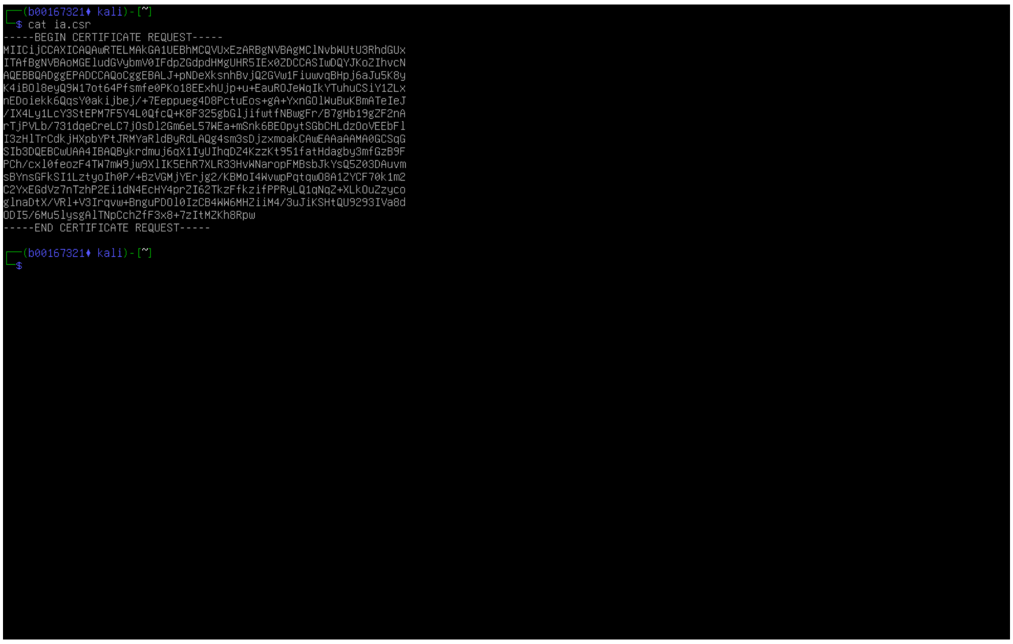
After generating the CSR, we can open it to view its encoded content

The CSR begins with

`-----BEGIN CERTIFICATE REQUEST---- -`

and ends with

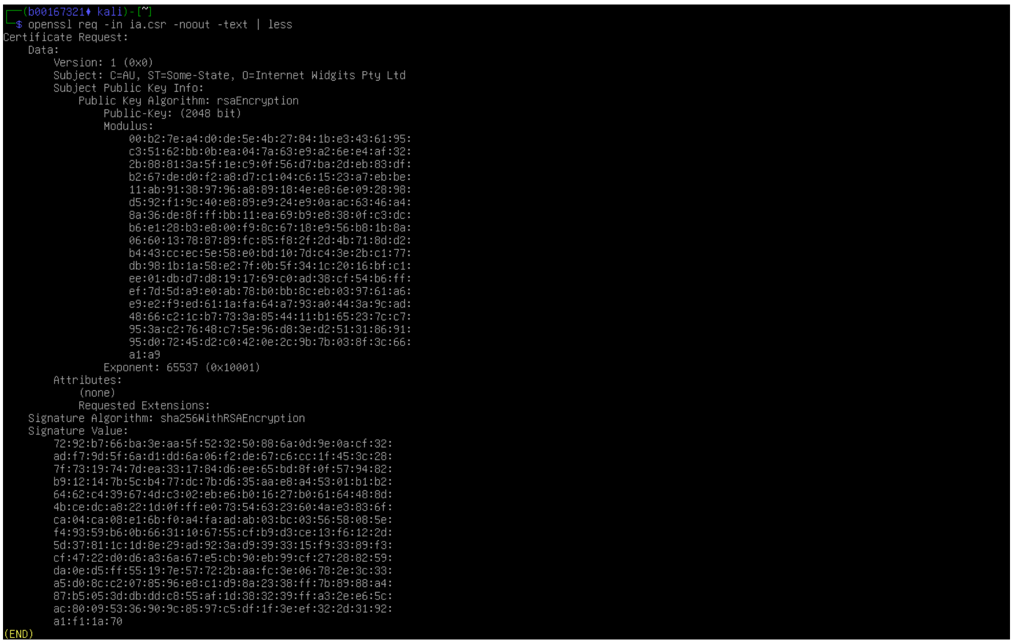
`-----END CERTIFICATE REQUEST-----`



```
┌──(b00167321♦ kali)-[~]
└─$ cat ia.csr
-----BEGIN CERTIFICATE REQUEST-----
MIICijCCAXICAQAwRTELMAkGA1UEBhMCQVUxEzARBgNVBAgMClNvbWUtU3RhdGUx
ITAfBgNVBAoMGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALJ+pNDeXksnhBvjQ2GVw1FiuwvqBHpj6aJu5K8y
K4iBOl8eyQ9W17ot64Pfsmfe0PKo18EExhUjp+u+EauROJeWqIkYTuhuCSiY1ZLx
nEDoiekk6QqsY0akijbej/+7Eeppueg4D8PctuEos+gA+YxnGOlWuBuKBmATeIeJ
/IX4Ly1LcY3StEPM7F5Y4L0QfcQ+K8F325gbGljifwtfNBwgFr/B7gHb19gZF2nA
rTjPVLb/731dqeCreLC7jOsDl2Gm6eL57WEa+mSnk6BEOpytSGbCHLdzOoVEEbFl
I3zHlTrCdkjHXpbYPtJRMYaRldByRdLAQg4sm3sDjzxmoakCAwEAAaAAMA0GCSqG
SIb3DQEBCwUAA4IBAQBykrdmuj6qX1IyUIhqDZ4KzzKt951fatHdagby3mfGzB9F
PCh/cxl0feozF4TW7mW9jw9XlIK5EhR7XLR33HvWNaropFMBsbJkYsQ5Z03DAuvm
sBYnsGFkSI1LztyoIh0P/+BzVGMjYErjg2/KBMoI4WvwpPqtqwO8A1ZYCF70k1m2
C2YxEGdVz7nTzhP2Ei1dN4EcHY4prZI62TkzFfkzifPPRyLQ1qNqZ+XLkOuZzyco
glnaDtX/VRl+V3Irqvw+BnguPDOl0IzCB4WW6MHZiiM4/3uJiKSHtQU9293IVa8d
ODI5/6Mu5lysgAlTNpCchZfF3x8+7zItMZKh8Rpw
-----END CERTIFICATE REQUEST-----

┌──(b00167321♦ kali)-[~]
└─$
```

Openssl: The OpenSSL command-line tool (used for cryptography, keys, and certificates)

- `Req`: This subcommand handles certificate requests (CSRs). It can both create and inspect them
- `-in ia.csr`: Tells OpenSSL to read input from the file ia.csr — our CSR file
- `-noout`: Means "don't output the encoded base64 content again." Without this, OpenSSL would print both the base64 data and the decoded info
- `-text`: Displays the decoded details of the CSR in a human-readable format



```
┌──(b00167321♦ kali)-[~]
└─$ openssl req -in ia.csr -noout -text | less
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b2:7e:a4:d0:de:5e:4b:27:84:1b:e3:43:61:95:
                    c3:51:62:bb:0b:ea:04:7a:63:e9:a2:6e:e4:af:32:
                    2b:88:81:3a:5f:1e:c9:0f:56:d7:ba:2d:eb:83:df:
                    b2:67:de:d0:f2:a8:d7:c1:04:c6:15:23:a7:eb:be:
                    11:ab:91:38:97:96:a8:89:18:4e:e8:6e:09:28:98:
                    d5:92:f1:9c:40:e8:89:e9:24:e9:0a:ac:63:46:a4:
                    8a:36:de:8f:ff:bb:11:ea:69:b9:e8:38:0f:c3:dc:
                    b6:e1:28:b3:e8:00:f9:8c:67:18:e9:56:b8:1b:8a:
                    06:60:13:78:87:89:fc:85:f8:2f:2d:4b:71:8d:d2:
                    b4:43:cc:ec:5e:58:e0:bd:10:7d:c4:3e:2b:c1:77:
                    db:98:1b:1a:58:e2:7f:0b:5f:34:1c:20:16:bf:c1:
                    ee:01:db:d7:d8:19:17:69:c0:ad:38:cf:54:b6:ff:
                    ef:7d:5d:a9:e0:ab:78:b0:bb:8c:eb:03:97:61:a6:
                    e9:e2:f9:ed:61:1a:fa:64:a7:93:a0:44:3a:9c:ad:
                    48:66:c2:1c:b7:73:3a:85:44:11:b1:65:23:7c:c7:
                    95:3a:c2:76:48:c7:5e:96:d8:3e:d2:51:31:86:91:
                    95:d0:72:45:d2:c0:42:0e:2c:9b:7b:03:8f:3c:66:
                    a1:a9
                Exponent: 65537 (0x10001)
        Attributes:
            (none)
            Requested Extensions:
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        72:92:b7:66:ba:3e:aa:5f:52:32:50:88:6a:0d:9e:0a:cf:32:
        ad:f7:9d:5f:6a:d1:dd:6a:06:f2:de:67:c6:cc:1f:45:3c:28:
        7f:73:19:74:7d:ea:33:17:84:d6:ee:65:bd:8f:0f:57:94:82:
        b9:12:14:7b:5c:b4:77:dc:7b:d6:35:aa:e8:a4:53:01:b1:b2:
        64:62:c4:39:67:4d:c3:02:eb:e6:b0:16:27:b0:61:64:48:8d:
        4b:ce:dc:a8:22:1d:0f:ff:e0:73:54:63:23:60:4a:e3:83:6f:
        ca:04:ca:08:e1:6b:f0:a4:fa:ad:ab:03:bc:03:56:58:08:5e:
        f4:93:59:b6:0b:66:31:10:67:55:cf:b9:d3:ce:13:f6:12:2d:
        5d:37:81:1c:1d:8e:29:ad:92:3a:d9:39:33:15:f9:33:89:f3:
        cf:47:22:d0:d6:a3:6a:67:e5:cb:90:eb:99:cf:27:28:82:59:
        da:0e:d5:ff:55:19:7e:57:72:2b:aa:fc:3e:06:78:2e:3c:33:
        a5:d0:8c:c2:07:85:96:e8:c1:d9:8a:23:38:ff:7b:89:88:a4:
        87:b5:05:3d:db:dd:c8:55:af:1d:38:32:39:ff:a3:2e:e6:5c:
        ac:80:09:53:36:90:9c:85:97:c5:df:1f:3e:ef:32:2d:31:92:
        a1:f1:1a:70
(END)
```

→ **Shows:**

- **Subject information (organisation, common name)**

    - **Public Key (2048-bit RSA)**
    - **Signature (CSR signature)**
    - **Algorithm used**
    - **Proof the CSR was signed using ia.key**

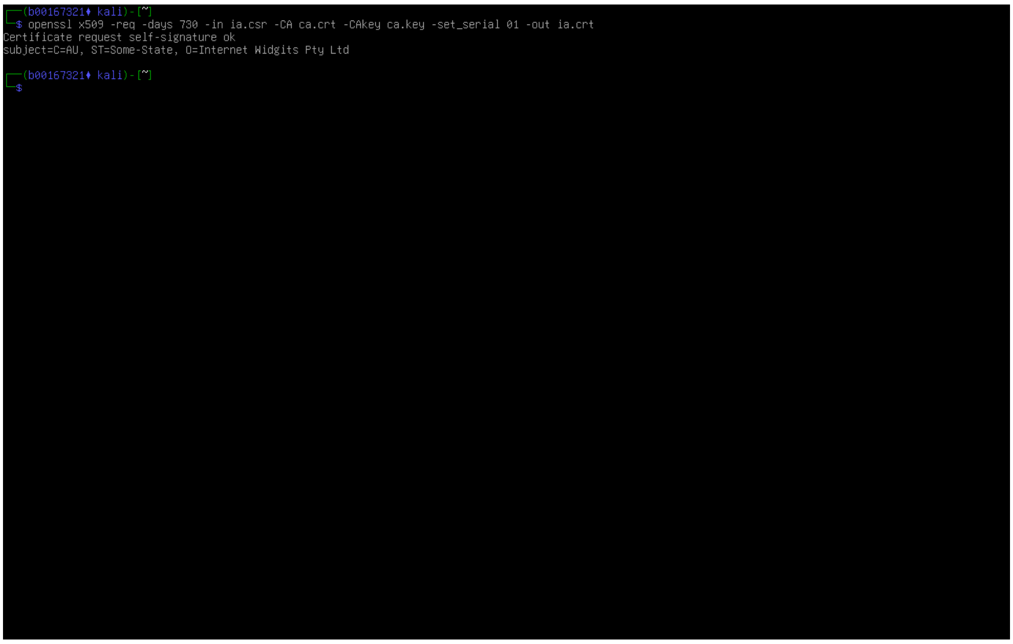
`-text` makes the CSR human-readable.

This confirms what information will appear in the issued certificate.

B.6 `openssl x509 -req -days 730 -in ia.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out ia.crt`

Use the <u>Root CA</u> to issue a certificate for the <u>Intermediate CA</u>

- `-req` → process a certificate signing request
- `-days 730` → validity period (2 years)
- `-CA & -CAkey` → specify the Root CA's certificate and private key
- `-out ia.crt` → output subordinate certificate



```
┌──(b00167321♦ kali)-[~]
└─$ openssl x509 -req -days 730 -in ia.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out ia.crt
Certificate request self-signature ok
subject=C=AU, ST=Some-State, O=Internet Widgits Pty Ltd

┌──(b00167321♦ kali)-[~]
└─$
```

→ **Output: ia.crt (Intermediate CA certificate)**

→ **Valid for 730 days (2 years)**

→ **Signed by the Root CA (ca.crt + ca.key)**

→ **The certificate now has:**

  - **Issuer: Root CA**
  - **Subject: Intermediate CA**

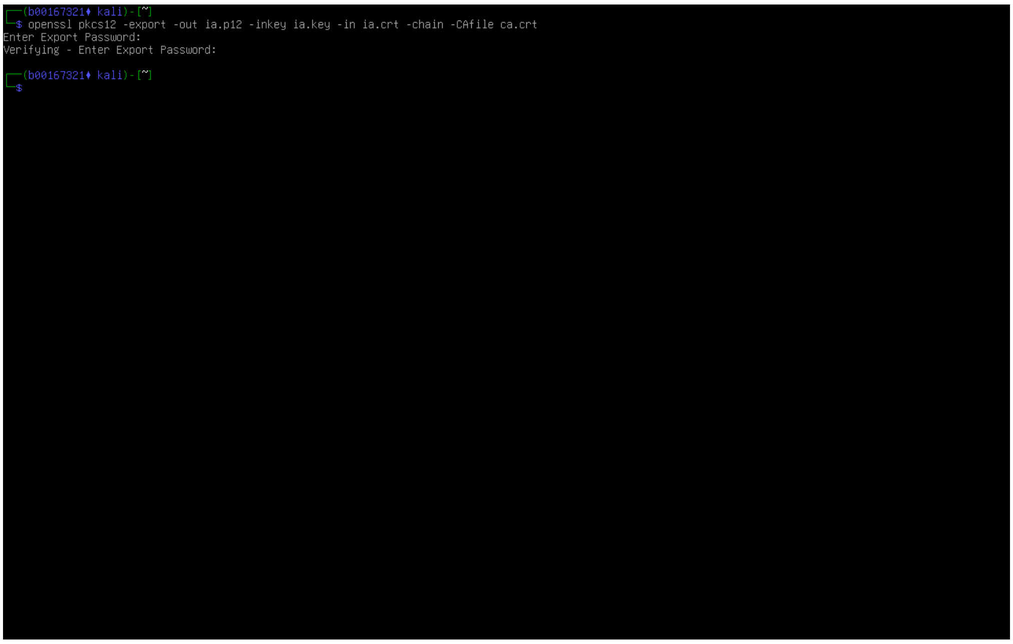
This step turns the CSR into a real certificate.

It is signed by the Root CA, establishing a trust chain.

B.7 `openssl pkcs12 -export -out ia.p12 -inkey ia.key -in ia.crt -chain -CAfile ca.crt`

To combine the key, certificate, and chain into a single file

- Used for digital signing and verification (e.g., code signing)
  - `ca.key`
  - `ca.crt`
  - `ia.key`
  - `ia.crt`



```
┌──(b00167321♦ kali)-[~]
└─$ openssl pkcs12 -export -out ia.p12 -inkey ia.key -in ia.crt -chain -CAfile ca.crt
Enter Export Password:
Verifying - Enter Export Password:

┌──(b00167321♦ kali)-[~]
└─$
```

→ **Created a file: ia.p12**

→ **Contains:**

- **Intermediate CA private key**
- **Intermediate CA certificate**
- **Root CA certificate (the chain)**

PKCS#12 files (.p12 or .pfx) are used for:

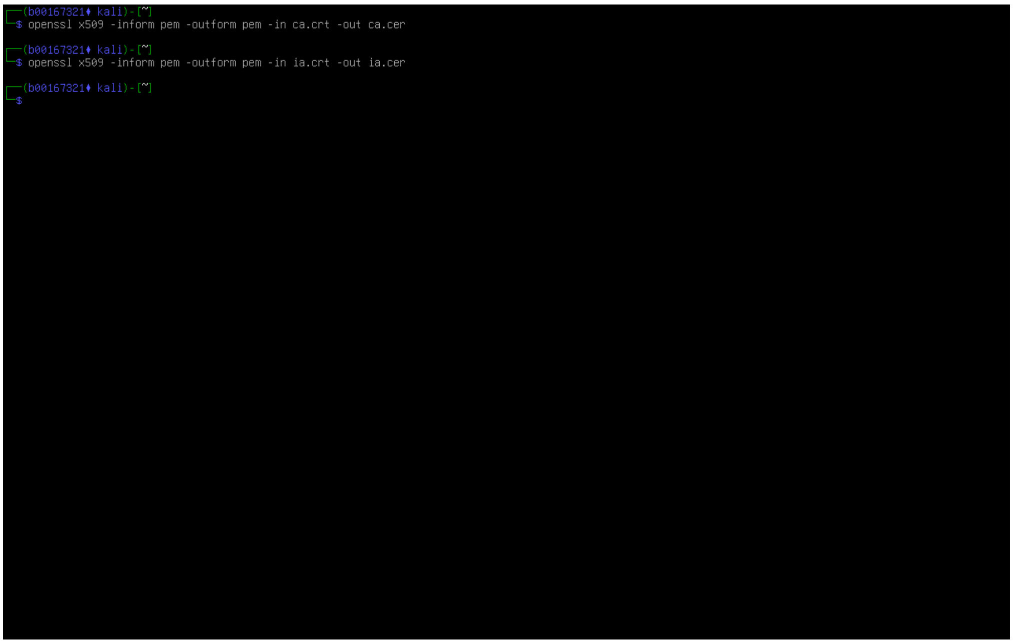
- Importing keys into browsers or servers
- Code signing
- TLS authentication

This bundles everything into one password-protected file.

B.8

```
openssl x509 -inform pem -outform pem -in ca.crt - out ca.cer
openssl x509 -inform pem -outform pem -in ia.crt - out ia.cer
```

Convert binary .crt to Base64 .cer for email or web use



```
┌──(b00167321♦ kali)-[~]
└─$ openssl x509 -inform pem -outform pem -in ca.crt -out ca.cer

┌──(b00167321♦ kali)-[~]
└─$ openssl x509 -inform pem -outform pem -in ia.crt -out ia.cer

┌──(b00167321♦ kali)-[~]
└─$
```

→ **ca.cer and ia.cer created in Base64 (PEM) format**

→ **These are easier to distribute or email**

→ **Same certificate data, different encoding**

PEM format (.cer) is Base64 encoded and includes the header lines:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

This makes the certificate readable and portable.

Lab 4: Trust and Digital Certificates

Objective: Digital certificates are used to define a trust infrastructure within PKI (Public Key Infrastructure). A certificate can hold a key pair, while a distributable certificate will only contain the public key. In this lab we will read-in digital certificates and analyse them.

🕮 **Lab demo:** https://youtu.be/-uNQFv0GTZc

A Introduction

No	Description	Result
A.1	From: 🕮 **Web link (Digital Certificate):** `http://asecuritysite.com/encryption/digitalcert` Open up Certificate 1 and identify the following:	Serial number: 702958 Effective date: 4/24/2008 8:18:42 PM Name: CN=Fred Smith, OU=None, E=fred@home, O=Nowhere, L=Edinburgh, S=Lothian, C=GB Issuer: CN=Fred Smith, OU=None, E=fred@home, O=Nowhere, L=Edinburgh, S=Lothian, C=GB What is CN used for: The Common Name – the primary name of the certificate holder, typically the domain name or person's name What is ON used for: Organizational Unit – identifies the department or group within the organization What is O used for: Organization – the company or legal entity owning the certificate What is L used for: Locality – the city where the organization or certificate owner is located
A.2	Now open-up the ZIP file for the certificate (Certificate 3), and view the DER file.	What other information can you gain from the certificate: Signature Algorithm: sha256WithRSAEncryption Issuer: Google Trust Services LLC (GTS CA 1C3) Key Usage: Digital Signature Extended Key Usage: TLS Web Server Authentication What is the size of the public key: 256 bit Which hashing method has been used: SHA-256 Is the certificate trusted on your system: [Yes][No]
A.3	Make a connection to the **www.live.com** Web site: `openssl s_client -connect www.live.com:443`	Can you identify the certificate chain? Yes What is the subject on the certificate? subject=C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, CN=outlook.live.com Who is the issuer on the certificate? issuer=C=US, O=DigiCert Inc, CN=DigiCert Cloud Services CA-1
A.4	Google moved in July 2018 to mark sites as being insecure if they did not have a match between their digital certificate and the site. A scan, at the time, on health and social care sites from the following page showed problems in digital certificates: https://bit.ly/2EkUvX0	Outline three sites that still have problems with their digital certificate, and the reason for the problem (you perhaps should try Chrome to assess): https://www.capability-scotland.org.uk Expired: Sunday 13 November 2022 at 23:59:59 https://www.heartstroketayside.org.uk localhost (is not trusted) Root certificate authority https://www.travax.scot.nhs.uk Expired: Saturday 1 November 2025 at 14:57:22 Pick two sites that you feel are not setup properly for their digital certificate, and then run a scan from SSLLabs (www.ssllabs.com). Identify the problems that they have with their digital certificate: https://www.capability-scotland.org.uk Sun, 13 Nov 2022 23:59:59 UTC (expired 2 years and 11 months ago) EXPIRED https://www.heartstroketayside.org.uk Alternative names – INVALID What are their SSLLabs rating? https://www.capability-scotland.org.uk T Rating https://www.heartstroketayside.org.uk T Rating Can you find a site with an "T" rating? Yes

A.5 Which the certificates in A.2, for Example 2 to Example 6. Complete the following table:

Cert	Organisation (Issued to)	Date range when valid	Size of public key	Issuer	Root CA	Hash method	Is it trusted?
2	No One / Nowhere Ltd (CN=No One)	Oct 29 2011 – Oct 28 2013	1024-bit RSA	No One (self-signed)	None (self-signed)	sha1WithRSAEncryptio	No
3	Google (CN=*.google.com)	Feb 08 2023 – May 03 2023	256-bit EC (P-256)	GTS CA 1C3	Google Trust Services Root	sha256WithRSAEncryption	No
4	Cisco Systems (CN=www.cisco.com)	Jul 10 2012 – Jul 11 2013	1024-bit RSA	VeriSign Class 3 Secure Server CA – G3	VeriSign Root	sha1WithRSAEncryption	No
5	Microsoft Corporation (CN=microsoft.com)	Jan 13 2023 – Jan 08 2024	2048-bit RSA	Microsoft Azure TLS Issuing CA 05	Microsoft Root CA	sha384WithRSAEncryption	No
6	Oracle Corporation (CN=oracle.com)	Feb 14 2023 – Feb 26 2024	2048-bit RSA	DigiCert TLS RSA SHA256 2020 CA1	DigiCert Root	sha256WithRSAEncryption	No

A.6 Now download the DER files from:

🕮 **Web link (Digital Certificate):** http://asecuritysite.com/der.zip

Now use openssl to read the certificates:

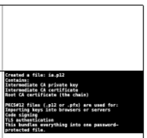
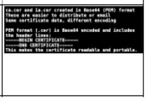
```
openssl x509 -inform der -in [certname] -noout -text
```

B Creating certificates

Now we will create our own self-signed certificates.

Step 1: Create a Private Key for the CA
Step 2: Create a Self-Signed Certificate for the CA (MegaCorp)
Step 3: Create a Subordinate (Intermediate) CA
Step 4: Generate a CSR for the Subordinate CA
Step 5: Inspect the CSR File
Step 6: Root CA Signs the Intermediate CA's CSR
Step 7: Create a PKCS#12 File for Signing
Step 8: Convert Between Formats

No	Description	Result
B.1	Create a Private Key for CA. Can do this using OpenSSL *openssl genrsa -out ca.key 2048* – genrsa → generates an RSA private key – -out ca.key → saves the key to a file named ca.key 2048 → key length in bits (can be 4096 for higher security)	A 2048-bit RSA private key stored in ca.key This key will be used to sign other certificates (it is the Root CA's private key) This command generates a new RSA private key for the Certificate Authority (CA). genrsa creates an unencrypted key, and -out ca.key saves it as a file
B.2	You can generate the certificate using **OpenSSL**: *openssl req -new -x509 -days 1826 -key ca.key -out ca.crt* **Explanation:** – req → create a certificate request – -new -x509 → generate a self-signed X.509 certificate – -days 1826 → certificate validity (5 years) – -key ca.key → use the private key created earlier -out ca.crt → output file (the new CA certificate)	Generated a self-signed CA certificate valid for 1826 days Output file: ca.crt This certificate includes the public key + issuer information This creates the Root Certificate. Because no external CA signs it, -x509 makes it self-signed, meaning it signs itself using ca.key.
B.3	You can generate a private key using **OpenSSL**: *openssl genrsa -out ia.key 2048* **Explanation:** – genrsa → generates an RSA private key – -out ia.key → saves the key to a file named *ia.key* – 2048 → key length in bits (can be 4096 for higher security)	Created a 2048-bit RSA private key for the intermediate authority File ia.key will be used to create a CSR next This is the private key for the subordinate CA, also called "Intermediate CA."
B.4	We now create a **Certificate Signing Request (CSR)** — a file containing identity details and the public key. *openssl req -new -key ia.key -out ia.csr* **Explanation:** • req -new → creates a new certificate request • -key ia.key → uses the subordinate CA's private key • -out ia.csr → saves the request in *ia.csr*	Output file: ia.csr Contains: Intermediate CA's public key Identity information Intended certificate fields A CSR is like an "application form" sent to a CA to request a certificate. It contains the public key and subject (organisation) information, but not a signature yet. A CSR is like an "application form" sent to a CA to request a certificate. It contains the public key and subject (organisation) information, but not a signature yet.
B.5	After generating the CSR, you can open it to view its encoded content: *cat ia.csr* **Explanation:** • The CSR begins with -----BEGIN CERTIFICATE REQUEST----- and ends with -----END CERTIFICATE REQUEST----- *openssl req -in ia.csr -noout -text* **Explanation:** Openssl: The OpenSSL command-line tool (used for cryptography, keys, and certificates). Req: This subcommand handles certificate requests (CSRs). It can both create and inspect them. -in ia.csr: Tells OpenSSL to read input from the file ia.csr — your CSR file. -noout: Means "don't output the encoded base64 content again." Without this, OpenSSL would print both the base64 data and the decoded info. -text: Displays the decoded details of the CSR in a human-readable format.	Shows: Subject information (organisation, common name) Public Key (2048-bit RSA) Signature (CSR signature) Algorithm used Proof the CSR was signed using ia.key -text makes the CSR human-readable. This confirms what information will appear in the issued certificate.
B.6	Use the **Root CA** to issue a certificate for the **Intermediate CA**: *openssl x509 -req -days 730 -in ia.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out ia.crt* **Explanation:** – -req → process a certificate signing request – -days 730 → validity period (2 years)	Output: ia.crt (Intermediate CA certificate) Valid for 730 days (2 years) Signed by the Root CA (ca.crt + ca.key) The certificate now has: Issuer: Root CA Subject: Intermediate CA This step turns the CSR into a real certificate. It is signed by the Root CA, establishing a trust chain.

	– -CA & -CAkey → specify the Root CA's certificate and private key – -out ia.crt → output subordinate certificate	
B.7	To combine the key, certificate, and chain into a single file: *openssl pkcs12 -export -out ia.p12 -inkey ia.key -in ia.crt -chain -CAfile ca.crt* • Used for **digital signing** and **verification** (e.g., code signing). – ca.key – **ca.crt** – ia.key – ia.crt	 Created a file: ia.p12 Contains: Intermediate CA private key Intermediate CA certificate Root CA certificate (the chain) PKCS#12 files (.p12 or .pfx) are used for: Importing keys into browsers or servers Code signing TLS authentication This bundles everything into one password-protected file.
B.8	Convert binary .crt to Base64 .cer for email or web use: *openssl x509 -inform pem -outform pem -in ca.crt -out ca.cer* *openssl x509 -inform pem -outform pem -in ia.crt -out ia.cer*	 ca.cer and ia.cer created in Base64 (PEM) format These are easier to distribute or email Same certificate data, different encoding PEM format (.cer) is Base64 encoded and includes the header lines: -----BEGIN CERTIFICATE----- -----END CERTIFICATE----- This makes the certificate readable and portable.

What I should have learnt from this lab?

The key things learnt:

- Understand how digital certificates are generated and ported onto systems.
- Identifying problems with digital certificates on sites.