National Australia Bank

GSE
GUIDE SHARE EUROPE
UK REGION

Digital Certificates

Principles of operation

Nigel Pentland

National Australia Group

February 2013

Nigel Pentland

Senior Security Analyst

nigel.pentland@eu.nabgroup.com

0141 223 3179

Digital Certificates

- Types of certificates
- Roles of certificates (identity, server, security & authentication)
- How is a certificate associated with something
- What are all the fields
- How are they managed with RACF
- Problem solving techniques - some scenarios and how to fix them with RACF commands
- How to set-up for the purpose of encrypting 3270 sessions, SSL sessions
- Discuss code from racf.co.uk

Types of certificates

- X.509
  - PKCS7 Cryptographic Message Syntax
  - PKCS10 Certification Request Syntax
  - PKCS11 Cryptographic Token Interface
  - PKCS12 Personal Information Exchange Syntax

Types of certificates

Vendor defined classes

VeriSign uses the concept of classes for different types of digital certificates:

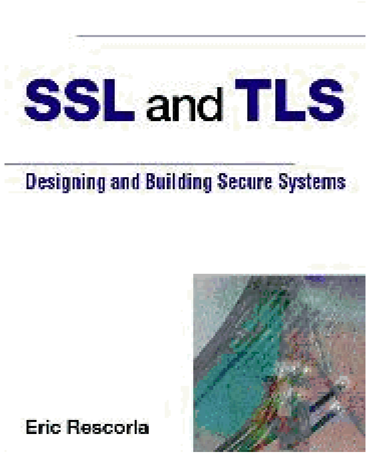
- Class 1 for individuals, intended for email.
- Class 2 for organizations, for which proof of identity is required.
- Class 3 for servers and software signing, for which independent verification and checking of identity and authority is done by the issuing certificate authority.
- Class 4 for online business transactions between companies.
- Class 5 for private organizations or governmental security.

Other vendors may choose to use different classes or no classes at all as this is not specified in the PKI standards.

Types of certificates

SSL and TLS certificates

http://www.rtfm.com/sslbook/

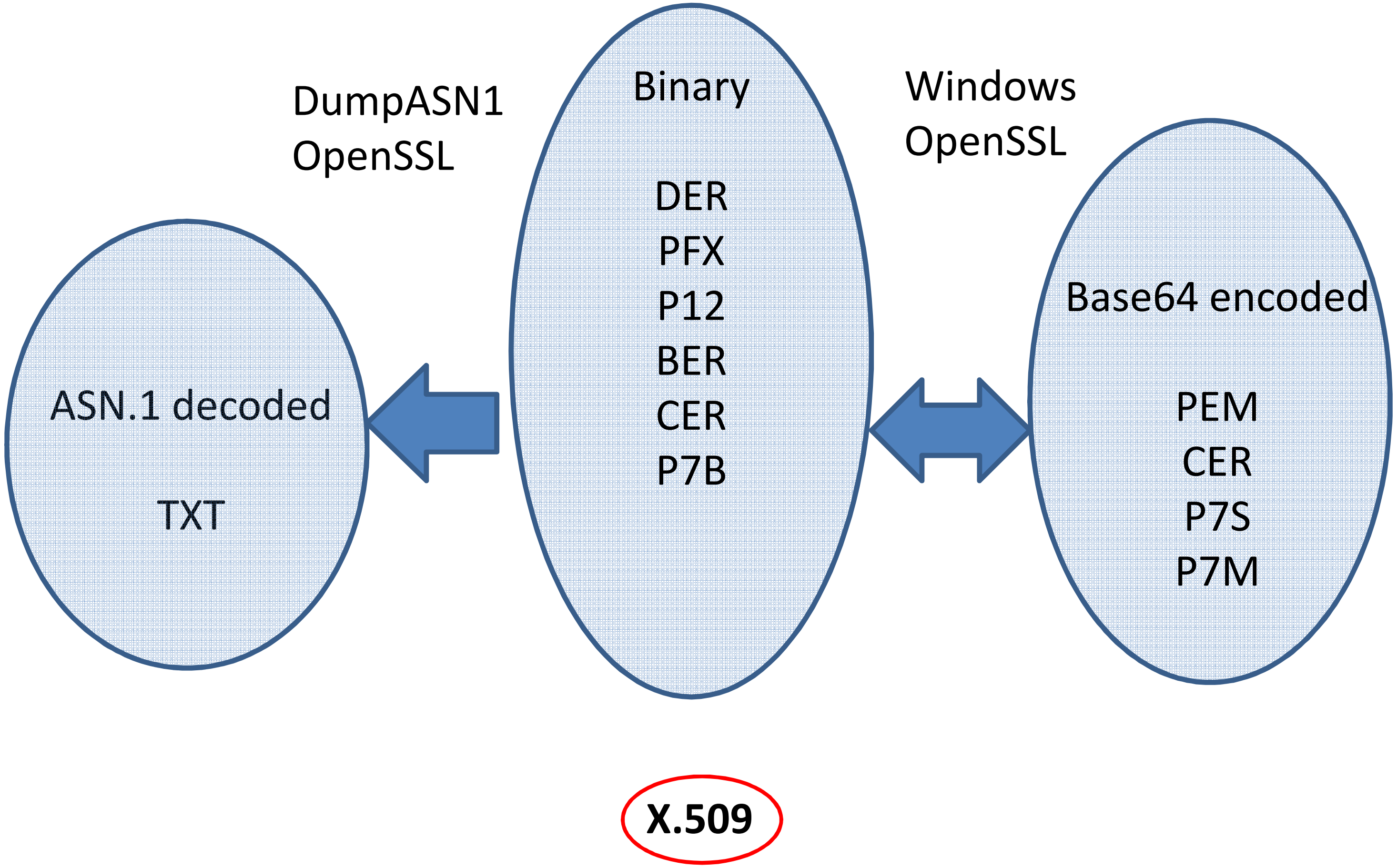


SSL and TLS

Designing and Building Secure Systems

Eric Rescorla

Types of certificates



TÜRK TRUST

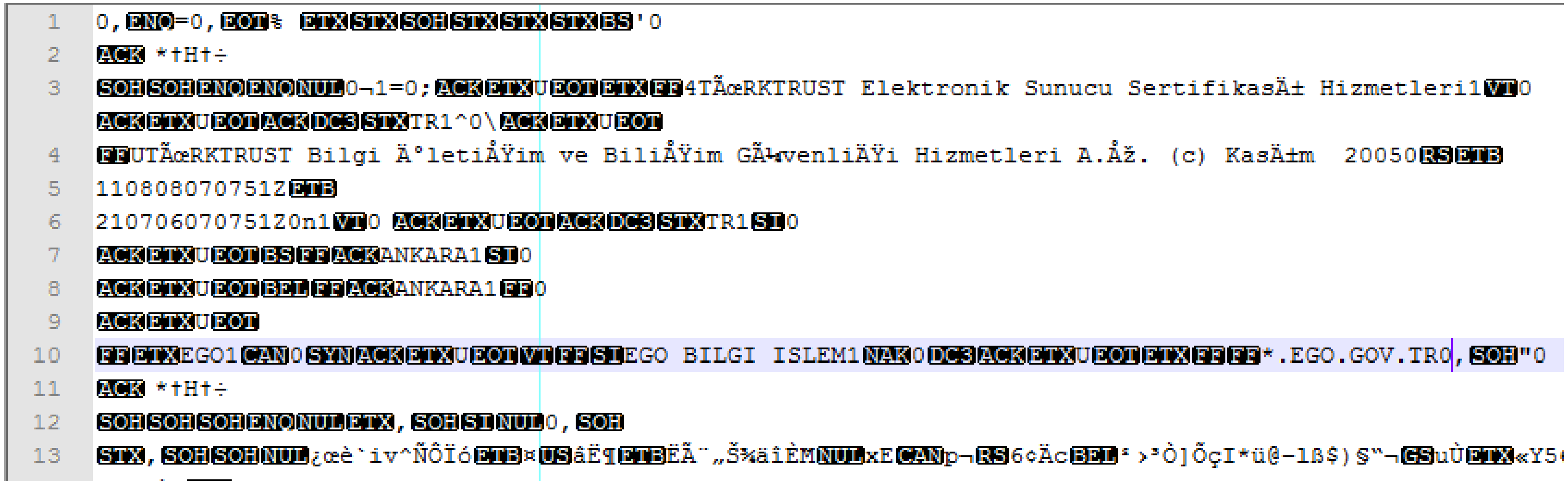
Topical example which is very much in the news

http://turktrust.com.tr/en/kamuoyu-aciklamasi-en.html

ASN.1

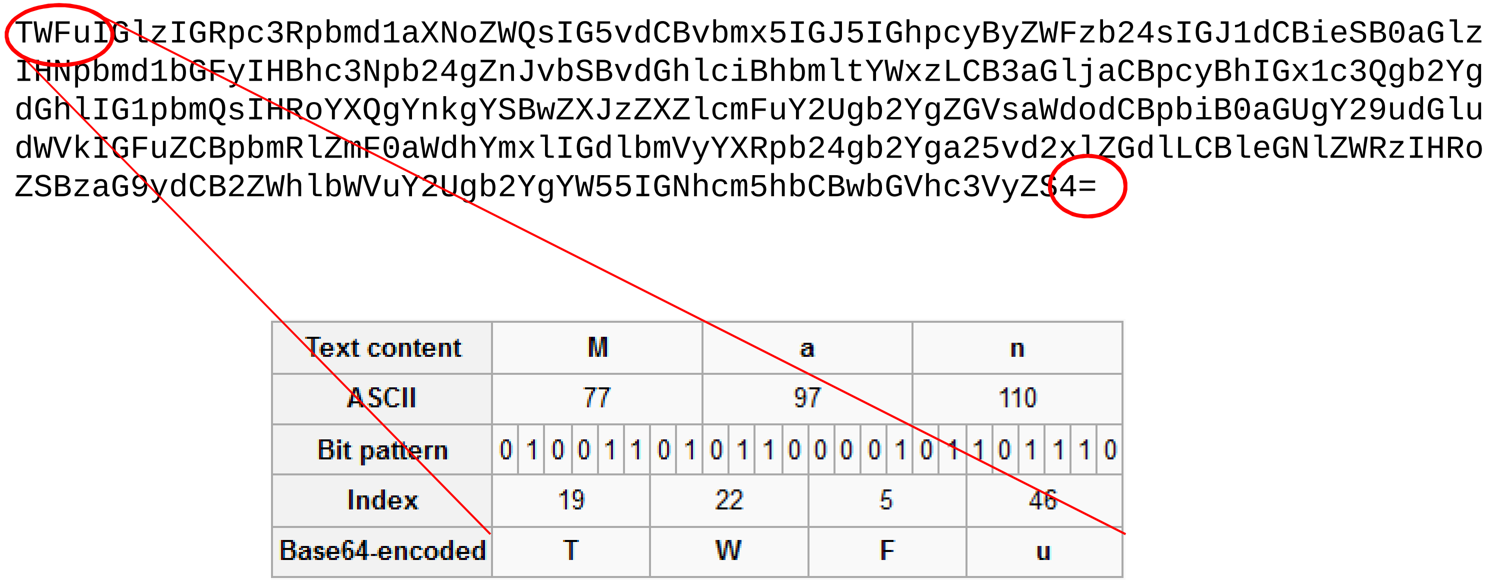
```
   0 1341: SEQUENCE {
   4 1061:   SEQUENCE {
   8    3:     [0] {
  10    1:       INTEGER 2
         :       }
  13    2:     INTEGER 2087
  17   13:     SEQUENCE {
  19    9:       OBJECT IDENTIFIER sha1withRSAEncryption (1 2 840 113549 1 1 5)
  30    0:       NULL
         :       }
  32  172:     SEQUENCE {
  35   61:       SET {
  37   59:         SEQUENCE {
  39    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
  44   52:           UTF8String
         :             'T..RKTRUST Elektronik Sunucu Sertifikas.. Hizmet'
         :             'leri'
         :           }
         :         }
  98   11:       SET {
 100    9:         SEQUENCE {
 102    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 107    2:           PrintableString 'TR'
         :           }
         :         }
 111   94:       SET {
```

Binary



```
0,ENQ=0,EOT% ETXSTXSOHSTXSTXSTXBS'0
ACK *†H†÷
SOHSOHENQENQNUL0¬1=0;ACKETXUEOTETXFF4TÃœRKTRUST Elektronik Sunucu SertifikasÄ± Hizmetleri1VT0
ACKETXUEOTACKDC3STXTR1^0\ACKETXUEOT
FFUTÃœRKTRUST Bilgi Ä°letiÅŸim ve BiliÅŸim GÃ¼venliÄŸi Hizmetleri A.Åž. (c) KasÄ±m  20050RSETB
110808070751ZETB
210706070751Z0n1VT0 ACKETXUEOTACKDC3STXTR1SI0
ACKETXUEOTBSFFACKANKARA1SI0
ACKETXUEOTBELFFACKANKARA1FF0
ACKETXUEOT
FFETXEGO1CAN0SYNACKETXUEOTVTFFSIEGO BILGI ISLEM1NAK0DC3ACKETXUEOTETXFFFF*.EGO.GOV.TR0,SOH"0
ACK *†H†÷
SOHSOHSOHENQNULETX,SOHSINUL0,SOH
STX,SOHSOHNUL¿œè`iv^ÑÔÏóETB¤USâË¶ETBËÃ¨„Š¾äîÈMNULxECANp¬RS6¢ÄcBEL² ›³Ò]ÕçI*ü@-1ß$)§"¬GSuÙETX«Y5
```

Base64



TWFuIGlzIGRpc3Rpbmd1aXNoZWQsIG5vdCBvbmx5IGJ5IGhpcyByZWFzb24sIGJ1dCBieSB0aGlz
IHNpbmd1bGFyIHBhc3Npb24gZnJvbSBvdGhlciBhbmltYWxzLCB3aGljaCBpcyBhIGx1c3Qgb2Yg
dGhlIG1pbmQsIHRoYXQgYnkgYSBwZXJzZXZlcmFuY2Ugb2YgZGVsaWdodCBpbiB0aGUgY29udGlu
dWVkIGFuZCBpbmRlZmF0aWdhYmxlIGdlbmVyYXRpb24gb2Yga25vd2xlZGdlLCBleGNlZWRzIHRo
ZSBzaG9ydCB2ZWhlbWVuY2Ugb2YgYW55IGNhcm5hbCBwbGVhc3VyZS4=

Text content	M								a								n							
ASCII	77								97								110							
Bit pattern	0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
Index	19						22						5						46					
Base64-encoded	T						W						F						u					

As this example illustrates, Base64 encoding converts 3 octets into 4 encoded characters.

http://www.fourmilab.ch/webtools/base64/

Types of certificates

- Certificate Authority
- Server side SSL
  - HTTP server
  - FTPS server (not SFTP)
  - TN3270 server
- S/MIME email certificate
- Client certificate
- Code Signing / Timestamping

Roles of certificates

(identity, server, security & authentication)

- Certificate Authority
  - Sign certificates
  - Sign CRLs / OCSP requests
- Server side certificates
  - Emphasis on DNS matching
  - Either Common Name (CN)
    - Or Subject Alternative Name (SAN)
- Client side certificates
  - Typically relies on Trust and Date only

How is a certificate associated with something

External packaging:

- Certificate label
- Certificate alias
- Key ring – either by certificate label or default

Internal property of certificate:

- Certificate Serial number
- Certificate Distinguished Name (DN)

What are all the fields

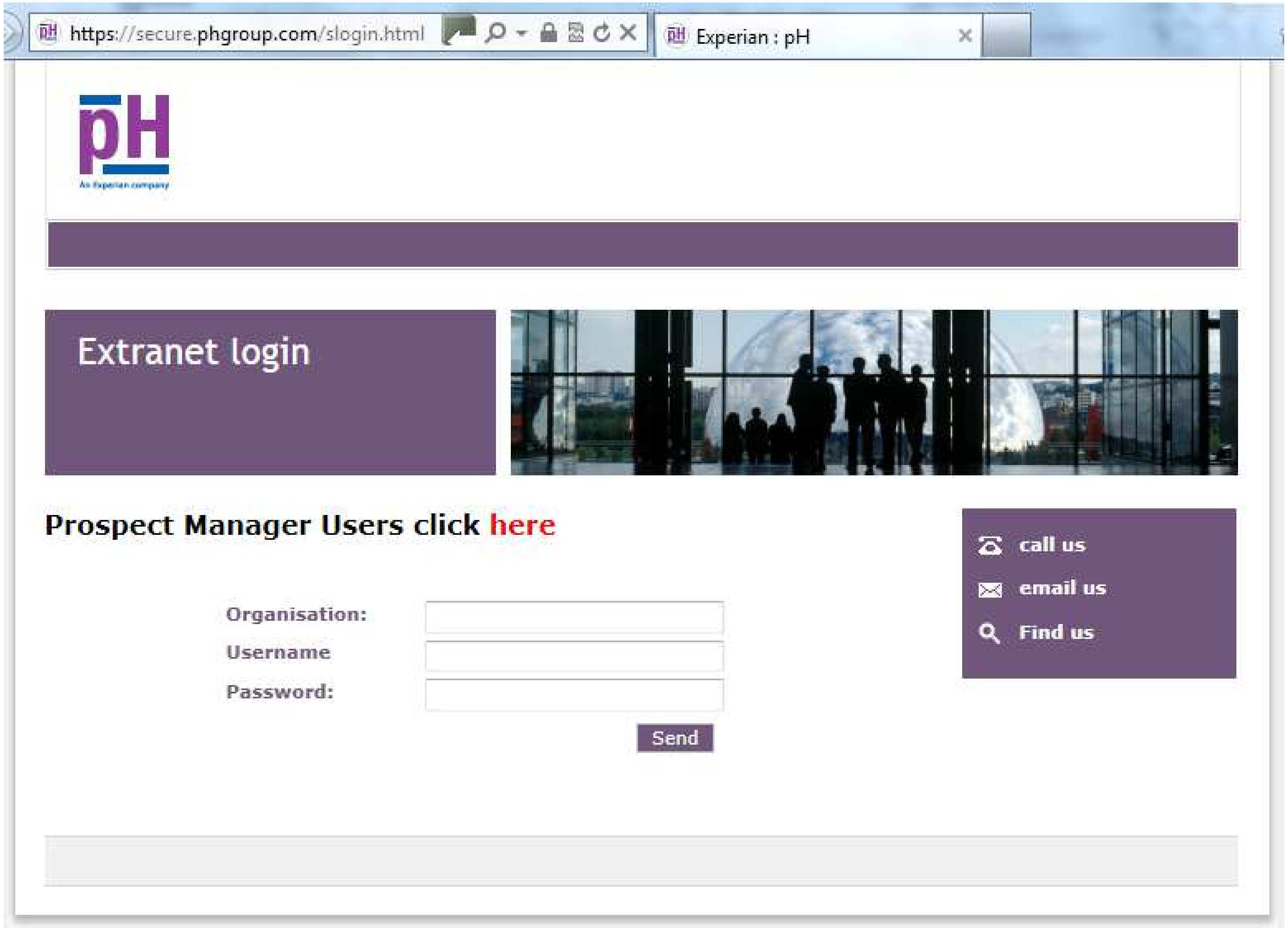
- Object Identifiers
  - **OID Repository** www.oid-info.com

OID Repository

http://oid-info.com

- OIDs
  - Well known OIDs
  - Less well know OIDs
    - Show up as string of numbers…

Examples



https://secure.phgroup.com/slogin.html

Experian : pH

pH

An Experian company

Extranet login

Prospect Manager Users click here

Organisation:

Username

Password:

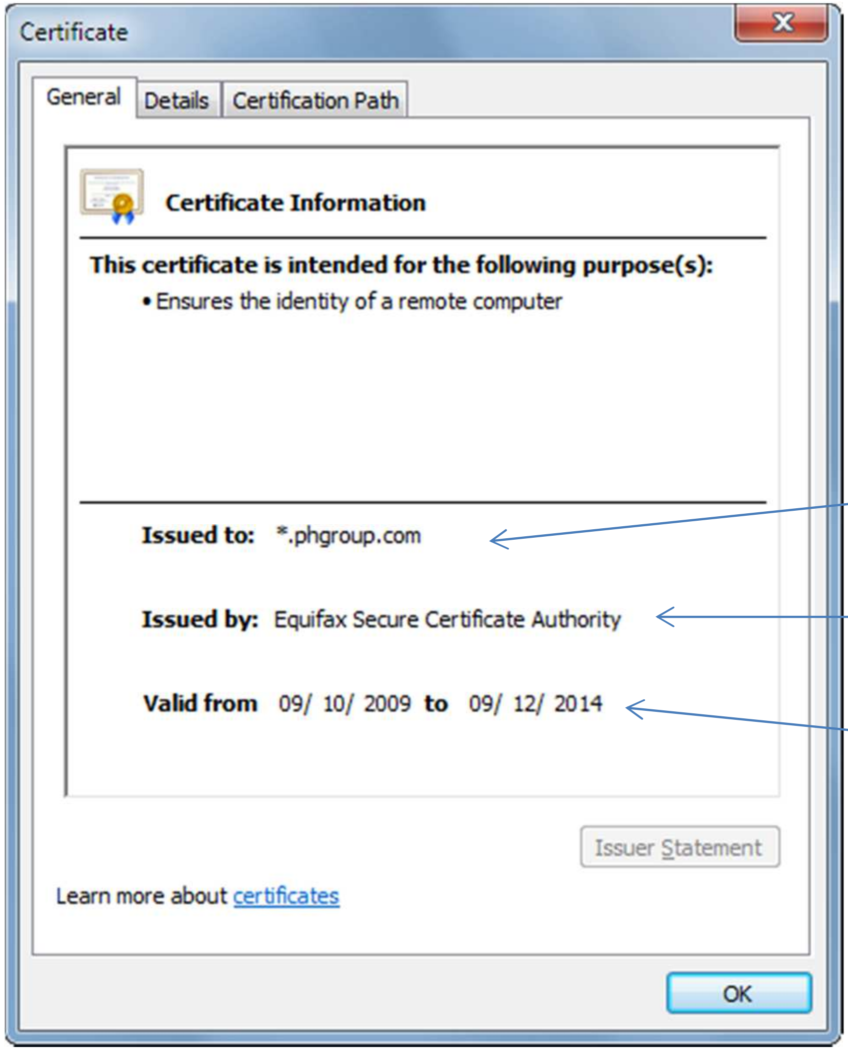
Send

☎ call us

✉ email us

Find us

Examples



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

Issued to: *.phgroup.com

Issued by: Equifax Secure Certificate Authority

Valid from 09/ 10/ 2009 **to** 09/ 12/ 2014

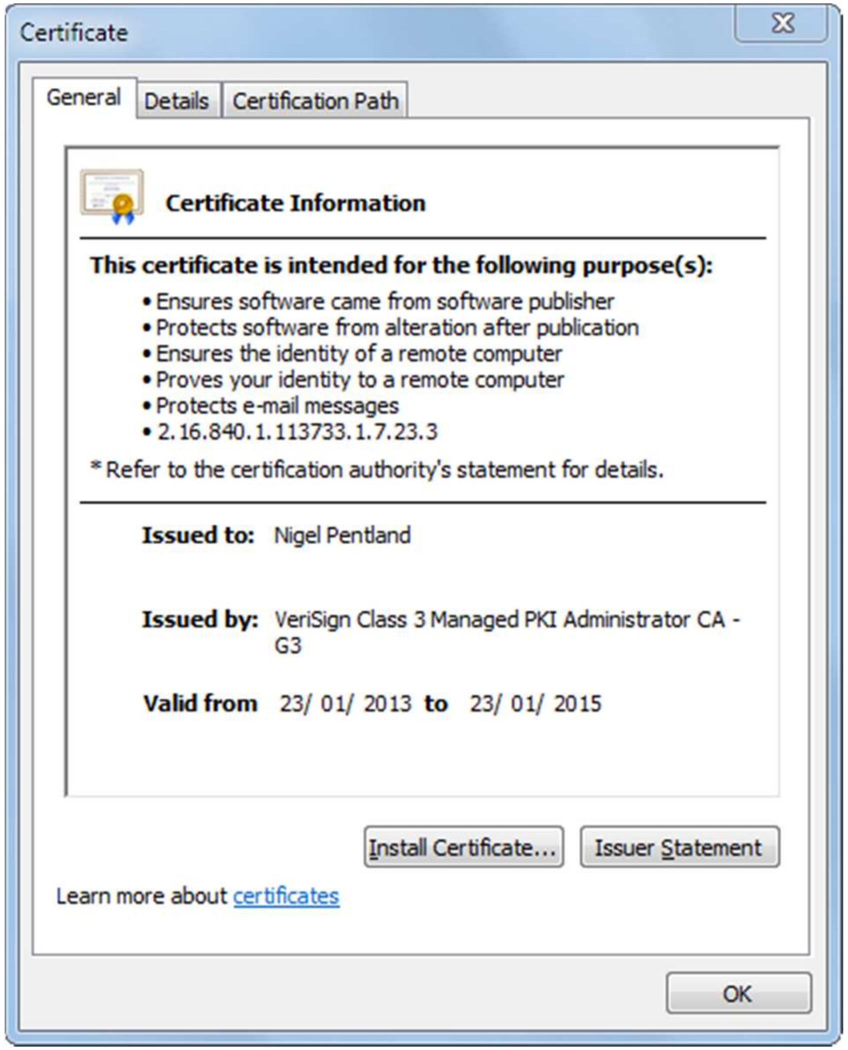
Wildcard certificate

Does URL match?

Is issuer trusted?

Is it within date?

Examples



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication
- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Protects e-mail messages
- 2.16.840.1.113733.1.7.23.3

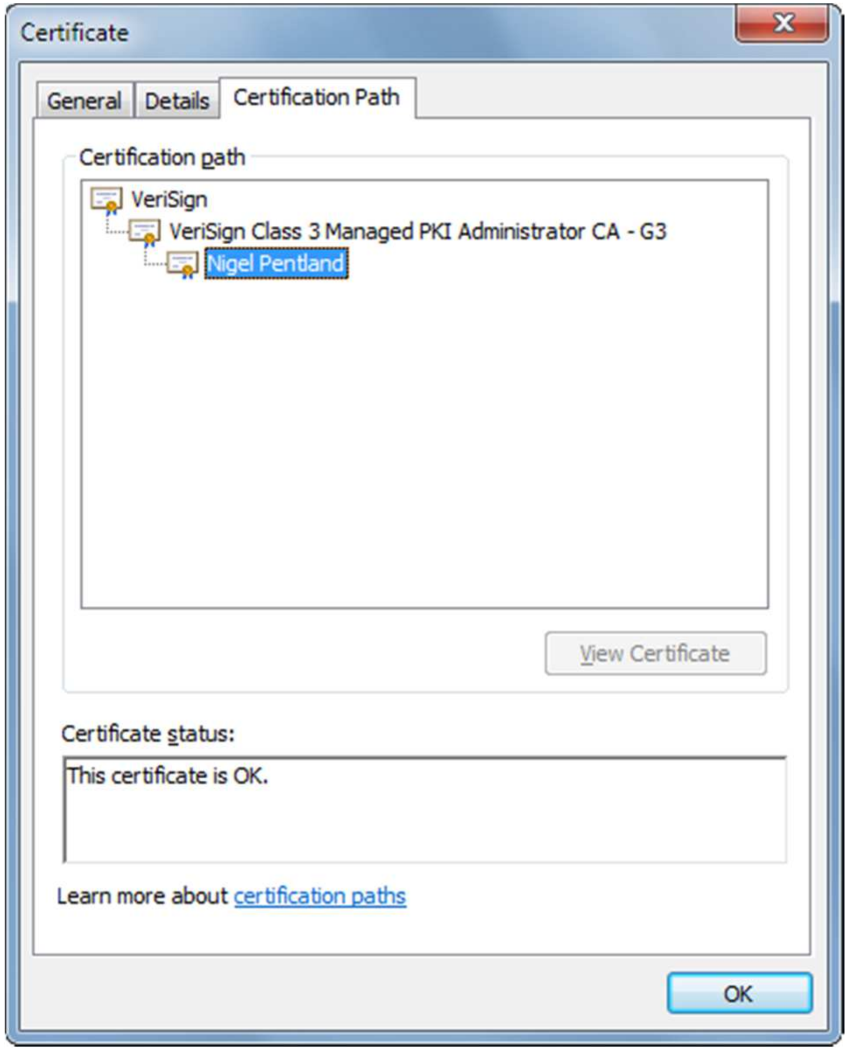
* Refer to the certification authority's statement for details.

Issued to: Nigel Pentland

Issued by: VeriSign Class 3 Managed PKI Administrator CA - G3

Valid from 23/ 01/ 2013 **to** 23/ 01/ 2015

Learn more about certificates



Certificate

Certification path

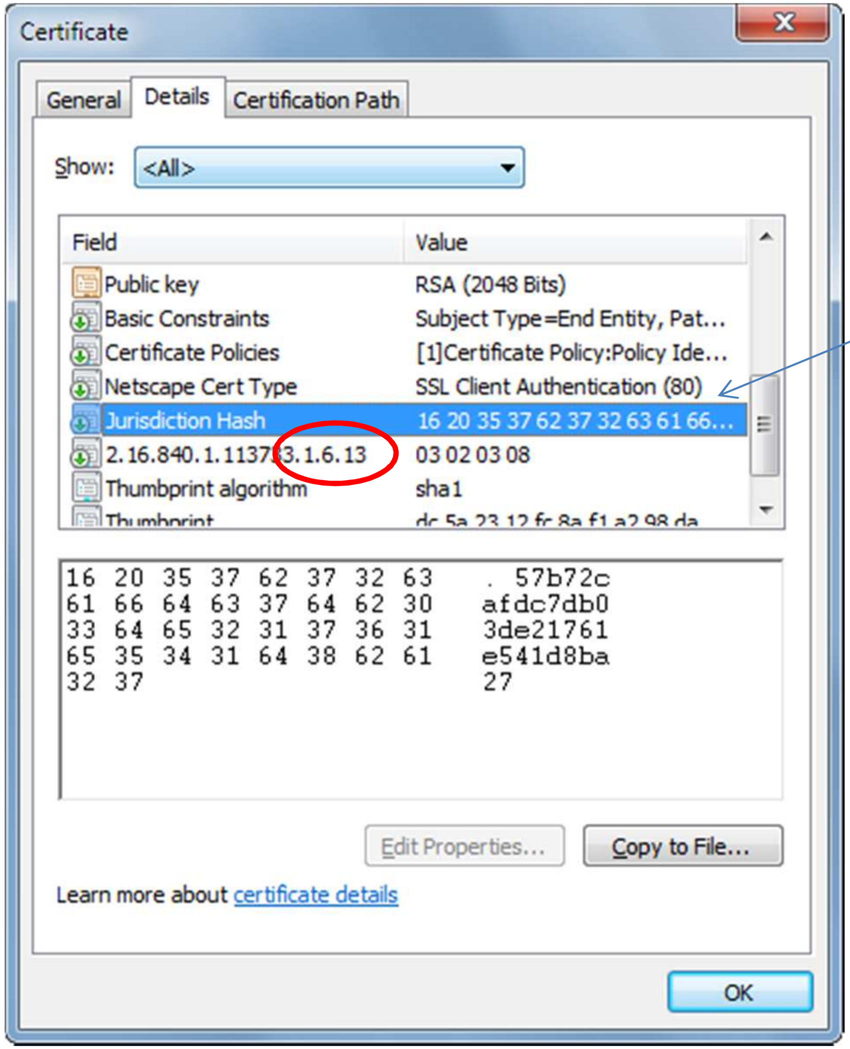
VeriSign
VeriSign Class 3 Managed PKI Administrator CA - G3
Nigel Pentland

Certificate status:

This certificate is OK.

Learn more about certification paths

Examples



Show: <All>

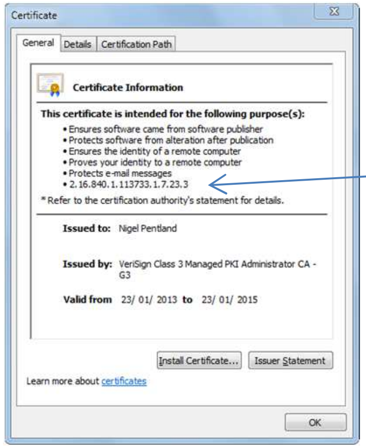
Field	Value
Public key	RSA (2048 Bits)
Basic Constraints	Subject Type=End Entity, Pat...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Netscape Cert Type	SSL Client Authentication (80)
Jurisdiction Hash	16 20 35 37 62 37 32 63 61 66...
2.16.840.1.113733.1.6.13	03 02 03 08
Thumbprint algorithm	sha1
Thumbprint	dc 5a 23 12 fc 8a f1 a2 98 da

```
16 20 35 37 62 37 32 63    . 57b72c
61 66 64 63 37 64 62 30   afdc7db0
33 64 65 32 31 37 36 31   3de21761
65 35 34 31 64 38 62 61   e541d8ba
32 37                     27
```

Learn more about certificate details

Appears as OID number in Windows XP

Examples



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication
- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Protects e-mail messages
- 2.16.840.1.113733.1.7.23.3

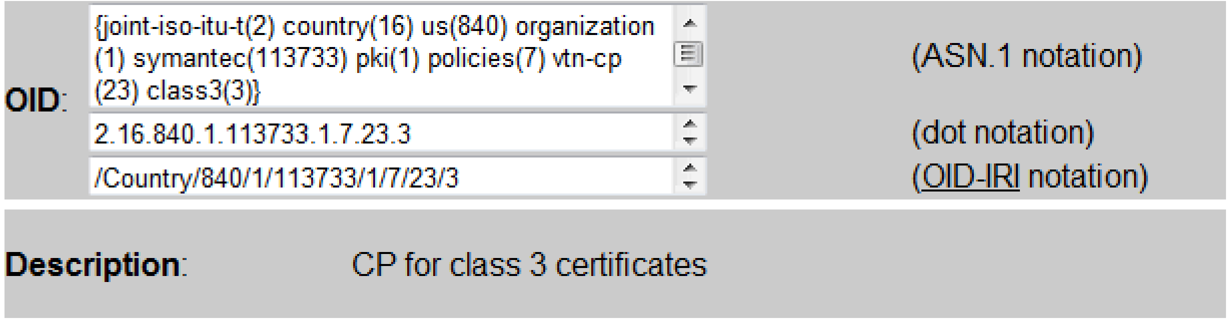
* Refer to the certification authority's statement for details.

Issued to: Nigel Pentland

Issued by: VeriSign Class 3 Managed PKI Administrator CA - G3

Valid from 23/ 01/ 2013 **to** 23/ 01/ 2015

Learn more about certificates

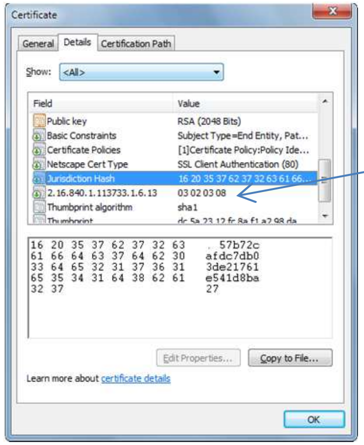


OID: {joint-iso-itu-t(2) country(16) us(840) organization (1) symantec(113733) pki(1) policies(7) vtn-cp (23) class3(3)} (ASN.1 notation)

2.16.840.1.113733.1.7.23.3 (dot notation)

/Country/840/1/113733/1/7/23/3 (OID-IRI notation)

Description: CP for class 3 certificates



Certificate

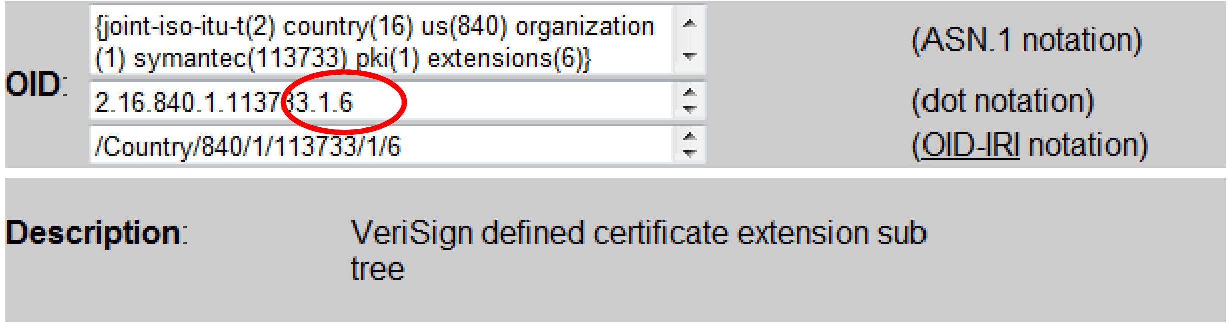
General | Details | Certification Path

Show: <All>

Field	Value
Public key	RSA (2048 Bits)
Basic Constraints	Subject Type=End Entity, Pat...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Netscape Cert Type	SSL Client Authentication (80)
Jurisdiction Hash	16 20 35 37 62 37 32 63 61 66...
2.16.840.1.113733.1.6.13	03 02 03 08
Thumbprint algorithm	sha1
Thumbprint	dc 5a 23 12 fc 8a f1 a2 98 da

```
16 20 35 37 62 37 32 63    . 57b72c
61 66 64 63 37 64 62 30    afdc7db0
33 64 65 32 31 37 36 31    3de21761
65 35 34 31 64 38 62 61    e541d8ba
32 37                      27
```

Learn more about certificate details



OID: {joint-iso-itu-t(2) country(16) us(840) organization (1) symantec(113733) pki(1) extensions(6)} (ASN.1 notation)

2.16.840.1.113733.1.6 (dot notation)

/Country/840/1/113733/1/6 (OID-IRI notation)

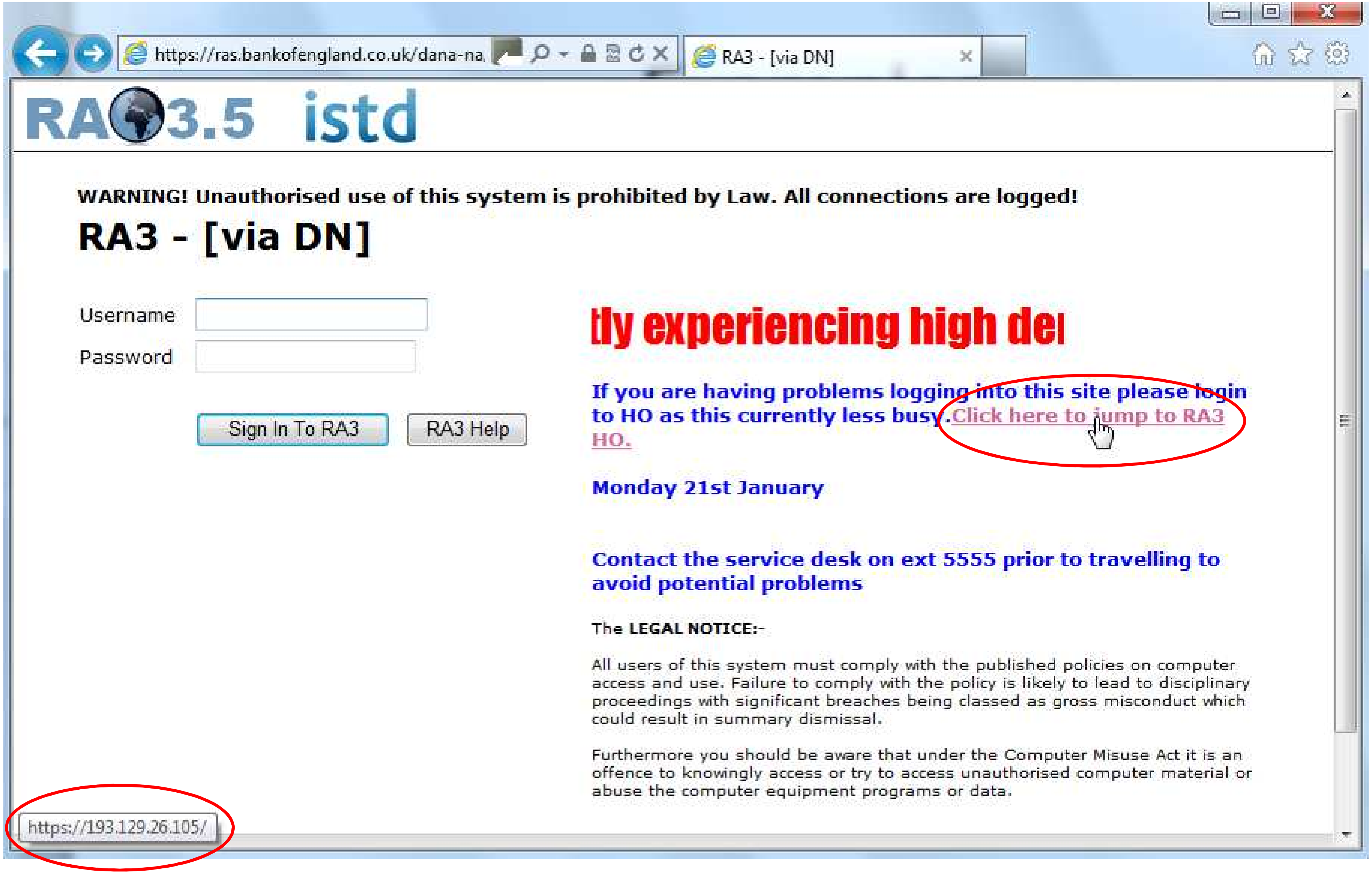
Description: VeriSign defined certificate extension sub tree

Examples

DumpASN1 output

```
806   48:          SEQUENCE {
808   10:            OBJECT IDENTIFIER
        :              verisignOnsiteJurisdictionHash (2 16 840 1 113733 1 6 11)
820   34:            OCTET STRING, encapsulates {
822   32:              IA5String '57b72cafdc7db03de21761e541d8ba27'
        :              }
        :            }
856   18:          SEQUENCE {
858   10:            OBJECT IDENTIFIER
        :              Unknown Verisign VPN extension (2 16 840 1 113733 1 6 13)
870    4:            OCTET STRING, encapsulates {
872    2:              BIT STRING 3 unused bits
        :                '10000'B (bit 4)
        :              }
        :            }
```

Examples



WARNING! Unauthorised use of this system is prohibited by Law. All connections are logged!

RA3 - [via DN]

Username

Password

tly experiencing high de

If you are having problems logging into this site please login to HO as this currently less busy.Click here to jump to RA3 HO.

Monday 21st January

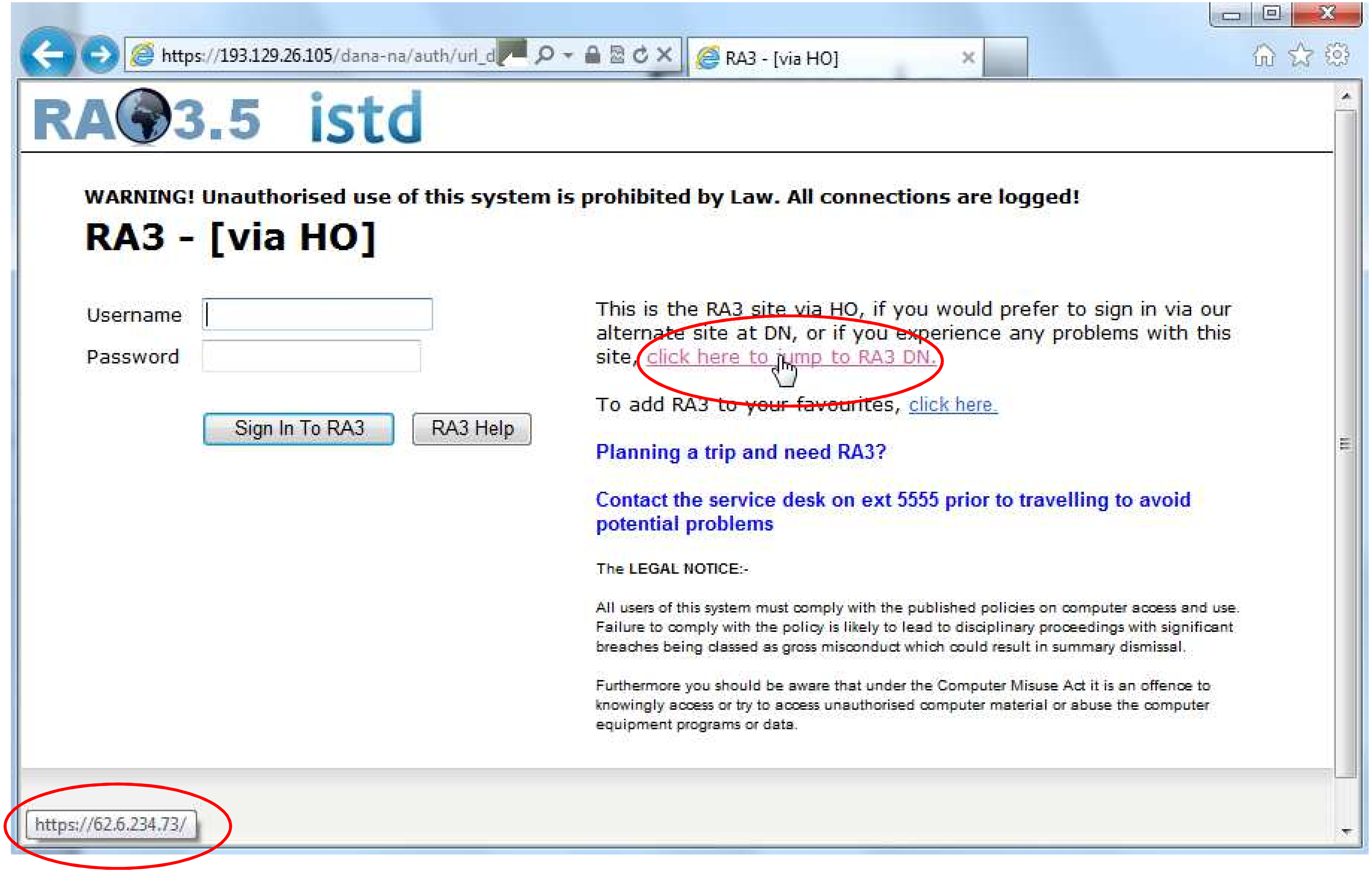
Contact the service desk on ext 5555 prior to travelling to avoid potential problems

The LEGAL NOTICE:-

All users of this system must comply with the published policies on computer access and use. Failure to comply with the policy is likely to lead to disciplinary proceedings with significant breaches being classed as gross misconduct which could result in summary dismissal.

Furthermore you should be aware that under the Computer Misuse Act it is an offence to knowingly access or try to access unauthorised computer material or abuse the computer equipment programs or data.

Examples



WARNING! Unauthorised use of this system is prohibited by Law. All connections are logged!

RA3 - [via HO]

Username

Password

This is the RA3 site via HO, if you would prefer to sign in via our alternate site at DN, or if you experience any problems with this site, click here to jump to RA3 DN.

To add RA3 to your favourites, click here.

Planning a trip and need RA3?

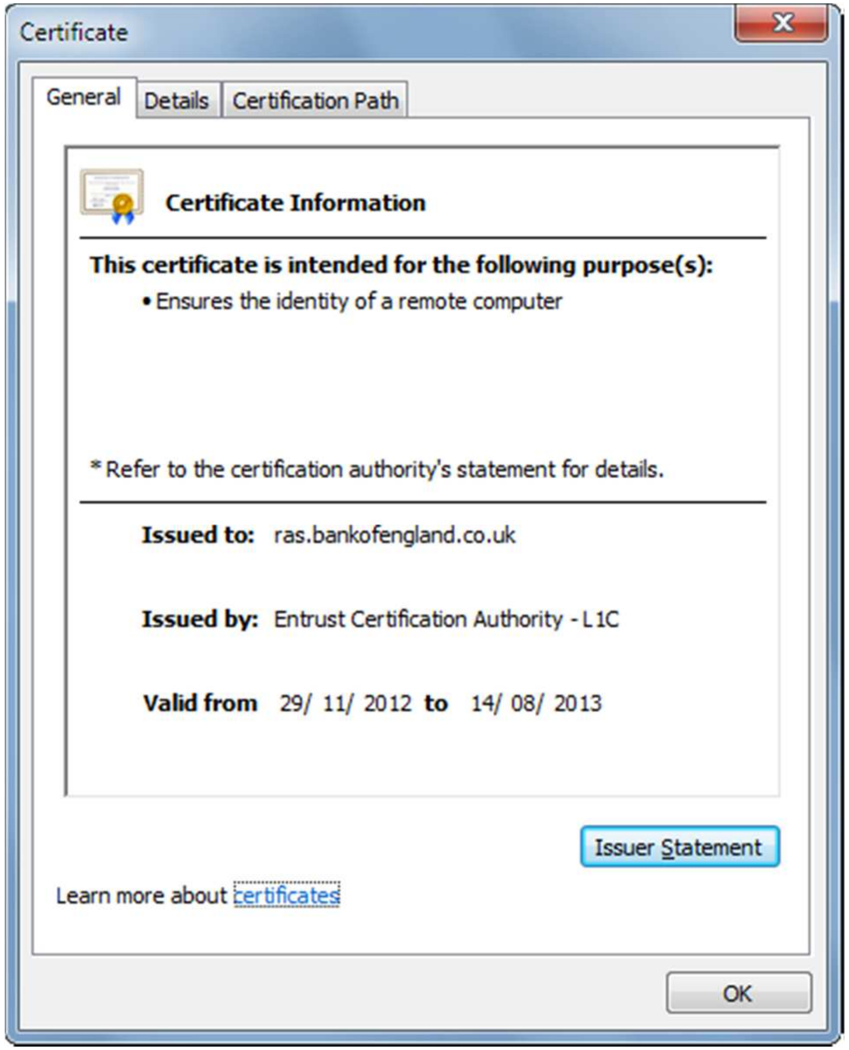
Contact the service desk on ext 5555 prior to travelling to avoid potential problems

The LEGAL NOTICE:-

All users of this system must comply with the published policies on computer access and use. Failure to comply with the policy is likely to lead to disciplinary proceedings with significant breaches being classed as gross misconduct which could result in summary dismissal.

Furthermore you should be aware that under the Computer Misuse Act it is an offence to knowingly access or try to access unauthorised computer material or abuse the computer equipment programs or data.

Examples



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

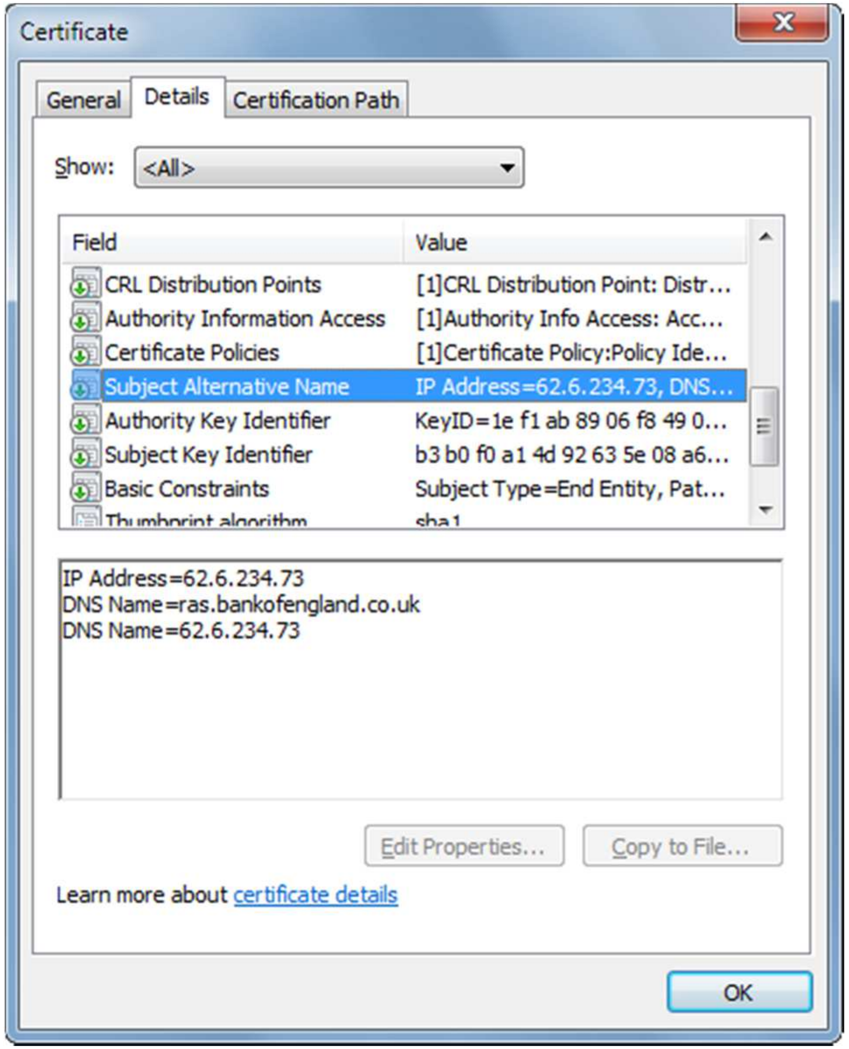
Issued to: ras.bankofengland.co.uk

Issued by: Entrust Certification Authority - L1C

Valid from 29/ 11/ 2012 **to** 14/ 08/ 2013

On the face of it,
it looks perfectly normal,
Or does it?

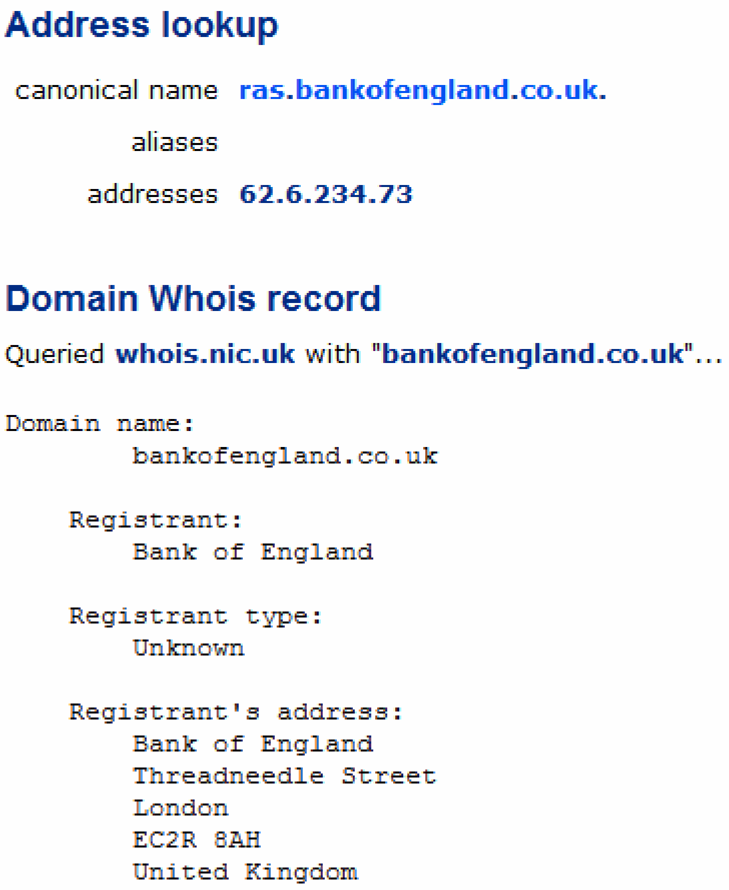
Examples



Field	Value
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Subject Alternative Name	IP Address=62.6.234.73, DNS...
Authority Key Identifier	KeyID=1e f1 ab 89 06 f8 49 0...
Subject Key Identifier	b3 b0 f0 a1 4d 92 63 5e 08 a6...
Basic Constraints	Subject Type=End Entity, Pat...
Thumbprint algorithm	sha1

IP Address=62.6.234.73
DNS Name=ras.bankofengland.co.uk
DNS Name=62.6.234.73

Learn more about certificate details



Address lookup

canonical name **ras.bankofengland.co.uk.**

aliases

addresses **62.6.234.73**

Domain Whois record

Queried **whois.nic.uk** with "**bankofengland.co.uk**"...

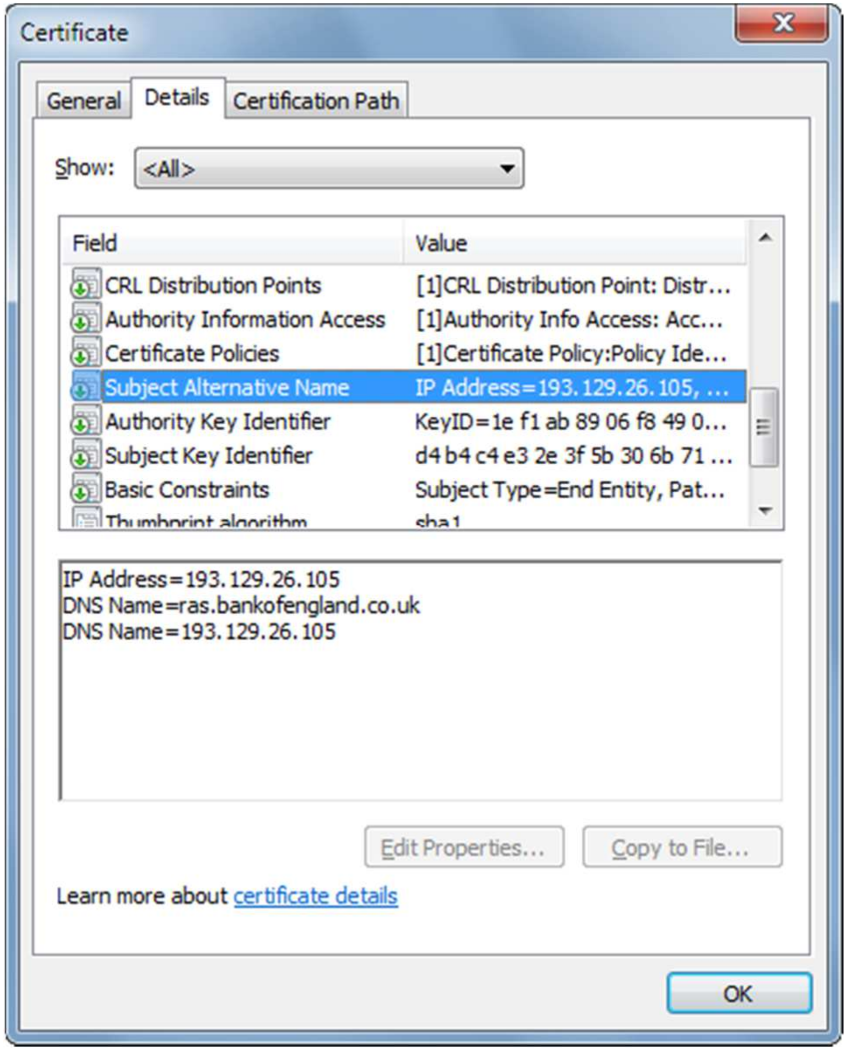
```
Domain name:
        bankofengland.co.uk

    Registrant:
        Bank of England

    Registrant type:
        Unknown

    Registrant's address:
        Bank of England
        Threadneedle Street
        London
        EC2R 8AH
        United Kingdom
```

Examples

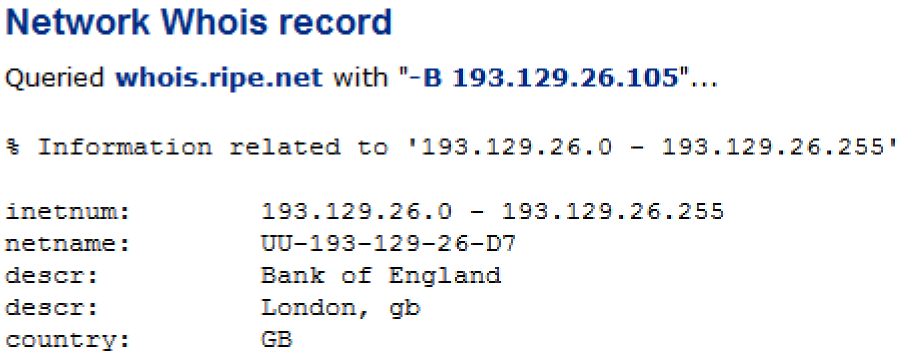


Show: <All>

Field	Value
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Subject Alternative Name	IP Address=193.129.26.105, ...
Authority Key Identifier	KeyID=1e f1 ab 89 06 f8 49 0...
Subject Key Identifier	d4 b4 c4 e3 2e 3f 5b 30 6b 71 ...
Basic Constraints	Subject Type=End Entity, Pat...
Thumbprint algorithm	sha1

IP Address=193.129.26.105
DNS Name=ras.bankofengland.co.uk
DNS Name=193.129.26.105

Learn more about certificate details



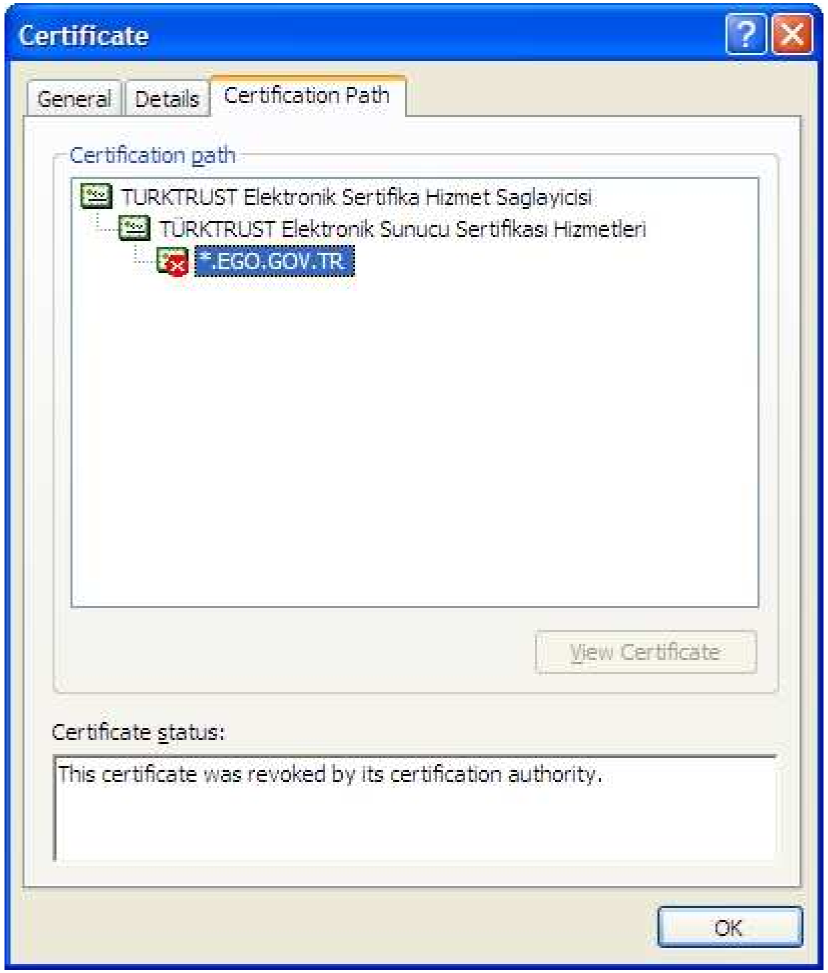
Network Whois record

Queried **whois.ripe.net** with "**-B 193.129.26.105**"...

```
% Information related to '193.129.26.0 - 193.129.26.255'

inetnum:        193.129.26.0 - 193.129.26.255
netname:        UU-193-129-26-D7
descr:          Bank of England
descr:          London, gb
country:        GB
```

Examples



Certification path

TURKTRUST Elektronik Sertifika Hizmet Saglayicisi
TÜRKTRUST Elektronik Sunucu Sertifikası Hizmetleri
*.EGO.GOV.TR

Certificate status:

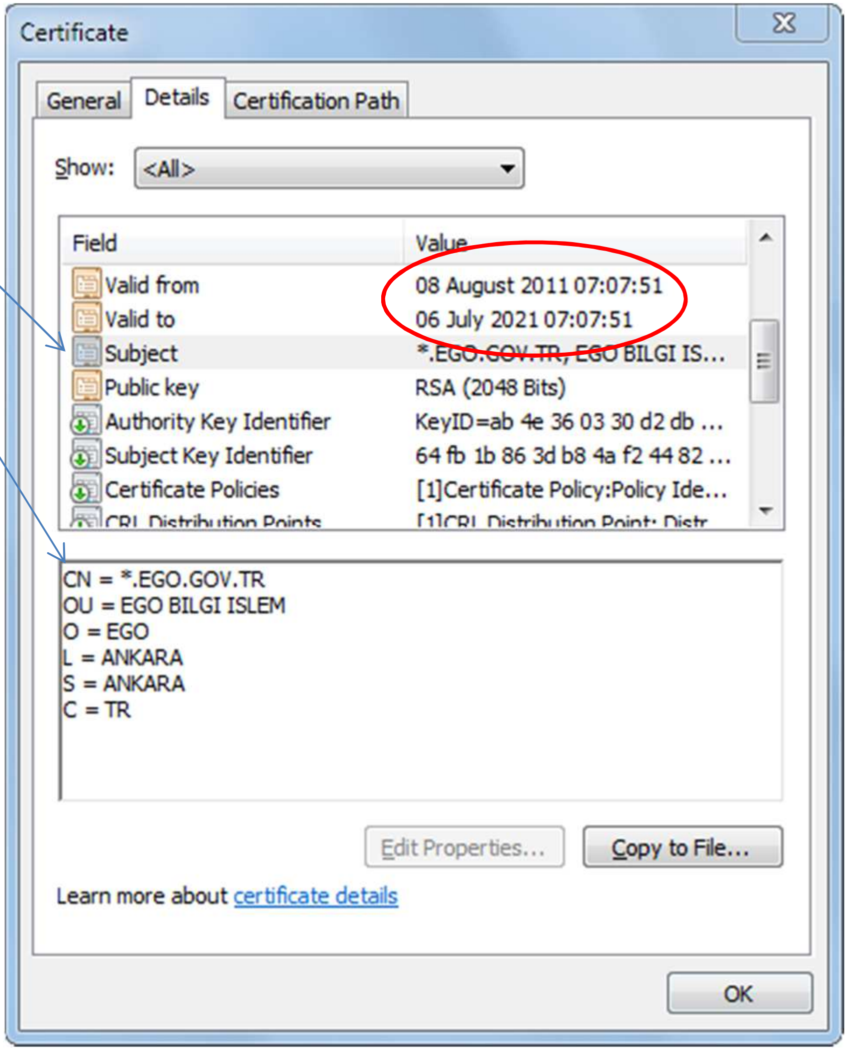
This certificate was revoked by its certification authority.

Certificate issued in error from TÜRK TRUST – interesting example, let's take a closer look…

Examples

Distinguished Name (DN)

```
239  110:     SEQUENCE {
241   11:       SET {
243    9:         SEQUENCE {
245    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
250    2:           PrintableString 'TR'
        :           }
        :         }
254   15:       SET {
256   13:         SEQUENCE {
258    3:           OBJECT IDENTIFIER stateOrProvinceName (2 5 4 8)
263    6:           UTF8String 'ANKARA'
        :           }
        :         }
271   15:       SET {
273   13:         SEQUENCE {
275    3:           OBJECT IDENTIFIER localityName (2 5 4 7)
280    6:           UTF8String 'ANKARA'
        :           }
        :         }
288   12:       SET {
290   10:         SEQUENCE {
292    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
297    3:           UTF8String 'EGO'
        :           }
        :         }
302   24:       SET {
304   22:         SEQUENCE {
306    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
311   15:           UTF8String 'EGO BILGI ISLEM'
        :           }
        :         }
328   21:       SET {
330   19:         SEQUENCE {
332    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
337   12:           UTF8String '*.EGO.GOV.TR'
        :           }
        :         }
        :       }
```



Show: <All>

Edit Properties...

Field	Value
Valid from	08 August 2011 07:07:51
Valid to	06 July 2021 07:07:51
Subject	*.EGO.GOV.TR, EGO BILGI IS...
Public key	RSA (2048 Bits)
Authority Key Identifier	KeyID=ab 4e 36 03 30 d2 db ...
Subject Key Identifier	64 fb 1b 86 3d b8 4a f2 44 82 ...
Certificate Policies	[1]Certificate Policy:Policy Ide...
CRL Distribution Points	[1]CRL Distribution Point: Distr

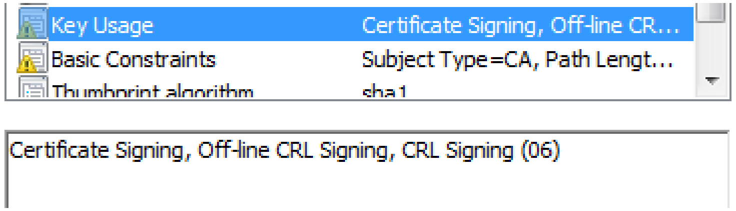
CN = *.EGO.GOV.TR
OU = EGO BILGI ISLEM
O = EGO
L = ANKARA
S = ANKARA
C = TR

Learn more about certificate details

Examples

```
717   14:          SEQUENCE {
719    3:            OBJECT IDENTIFIER keyUsage (2 5 29 15)
724    1:            BOOLEAN TRUE
727    4:            OCTET STRING, encapsulates {
729    2:              BIT STRING 1 unused bit
        :                '1100000'B
        :              }
        :            }
```

keyUsage



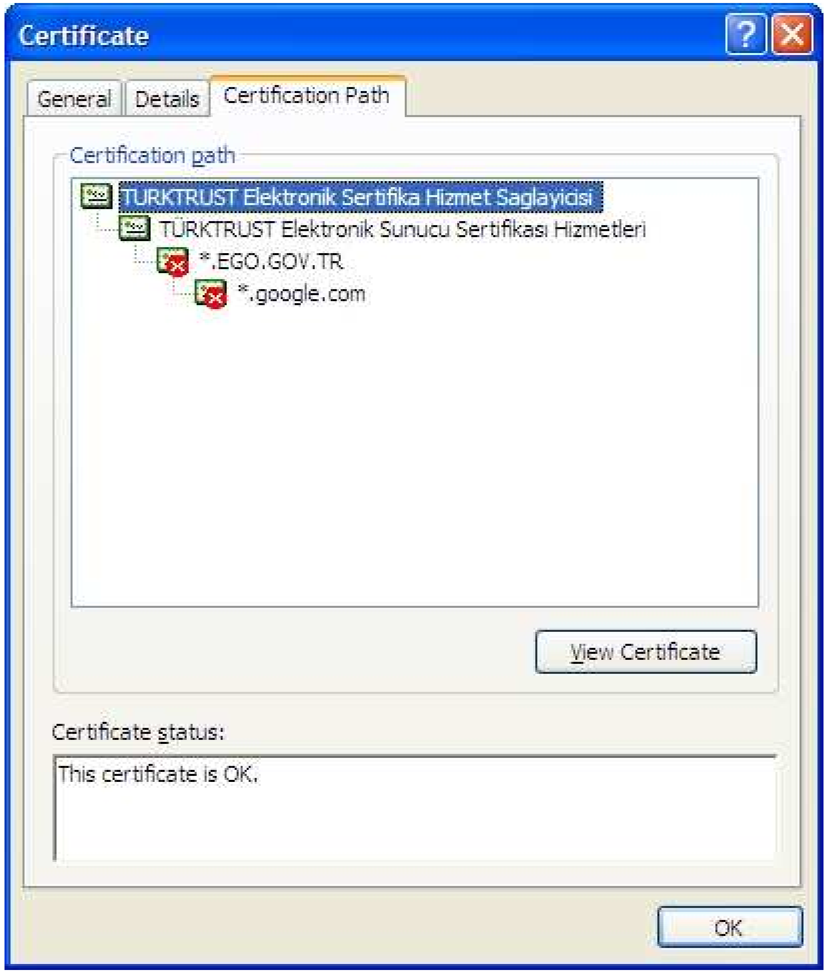
Key Usage   Certificate Signing, Off-line CR...
Basic Constraints   Subject Type=CA, Path Lengt...
Thumbprint algorithm   sha1

Certificate Signing, Off-line CRL Signing, CRL Signing (06)

AIA
authority Info Access

```
 896  170:          SEQUENCE {
 899    8:            OBJECT IDENTIFIER authorityInfoAccess (1 3 6 1 5 5 7 1 1)
 909  157:            OCTET STRING, encapsulates {
 912  154:              SEQUENCE {
 915  110:                SEQUENCE {
 917    8:                  OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
 927   98:                  [6]
          :                    'http://www.turktrust.com.tr/sertifikalar/TURKTRU'
          :                    'ST_Elektronik_Sunucu_Sertifikasi_Hizmetleri_s2.c'
          :                    'rt'
          :                  }
1027   40:                SEQUENCE {
1029    8:                  OBJECT IDENTIFIER ocsp (1 3 6 1 5 5 7 48 1)
1039   28:                  [6] 'http://ocsp.turktrust.com.tr'
          :                  }
          :                }
          :              }
          :            }
```

Examples

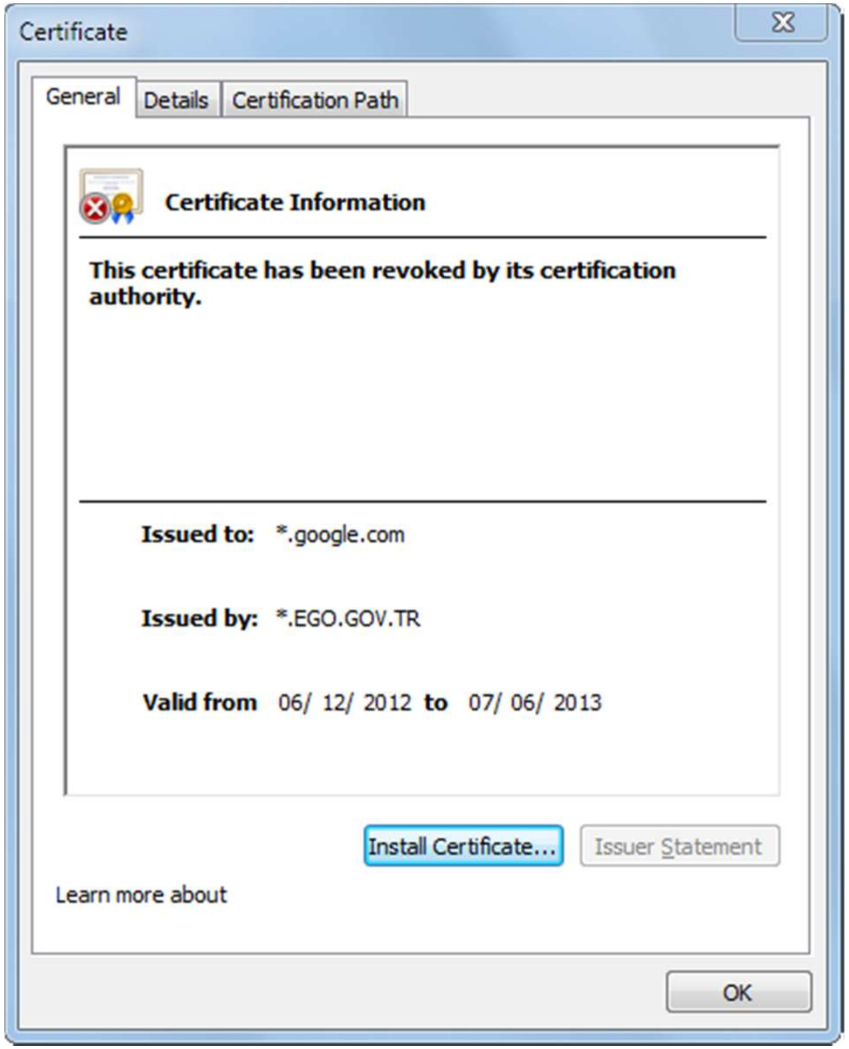


TURKTRUST Elektronik Sertifika Hizmet Saglayicisi
TÜRKTRUST Elektronik Sunucu Sertifikası Hizmetleri
*.EGO.GOV.TR
*.google.com

This certificate is OK.

Oops – looks like someone else has also noticed it can be used as a Certificate Authority and used to issue trusted certificates…

Examples



Certificate Information

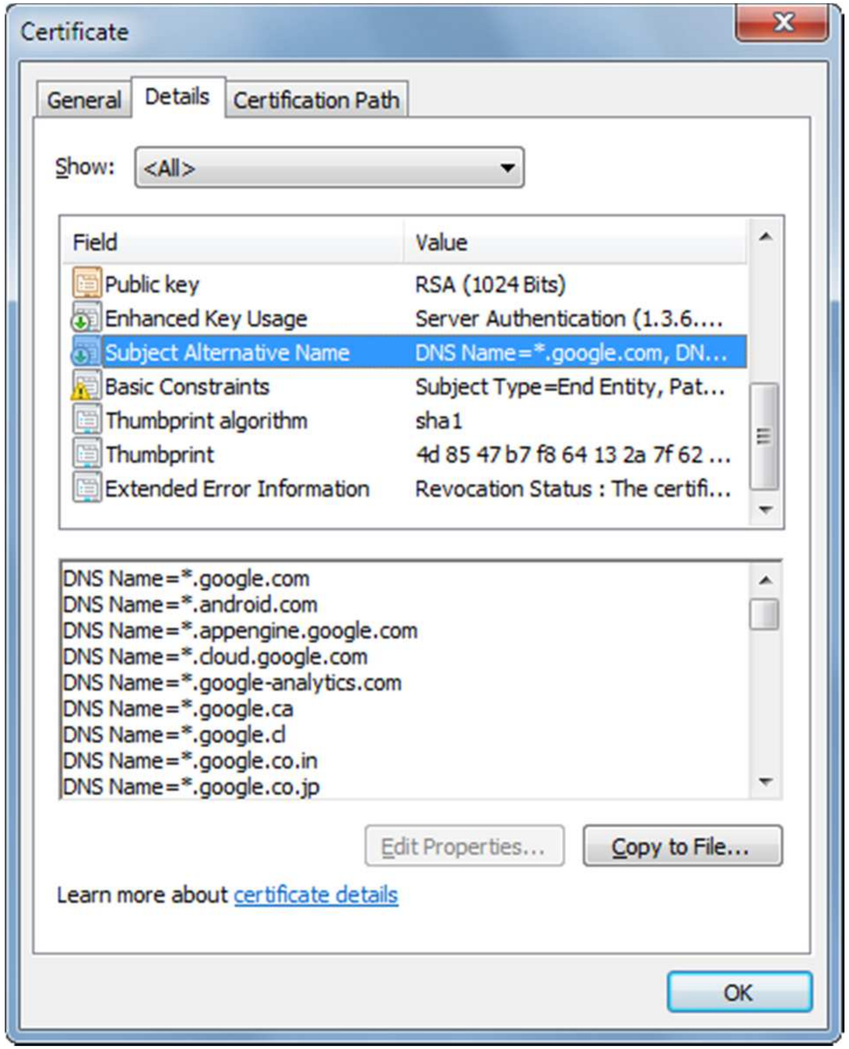
This certificate has been revoked by its certification authority.

Issued to: *.google.com

Issued by: *.EGO.GOV.TR

Valid from 06/ 12/ 2012 **to** 07/ 06/ 2013

Learn more about



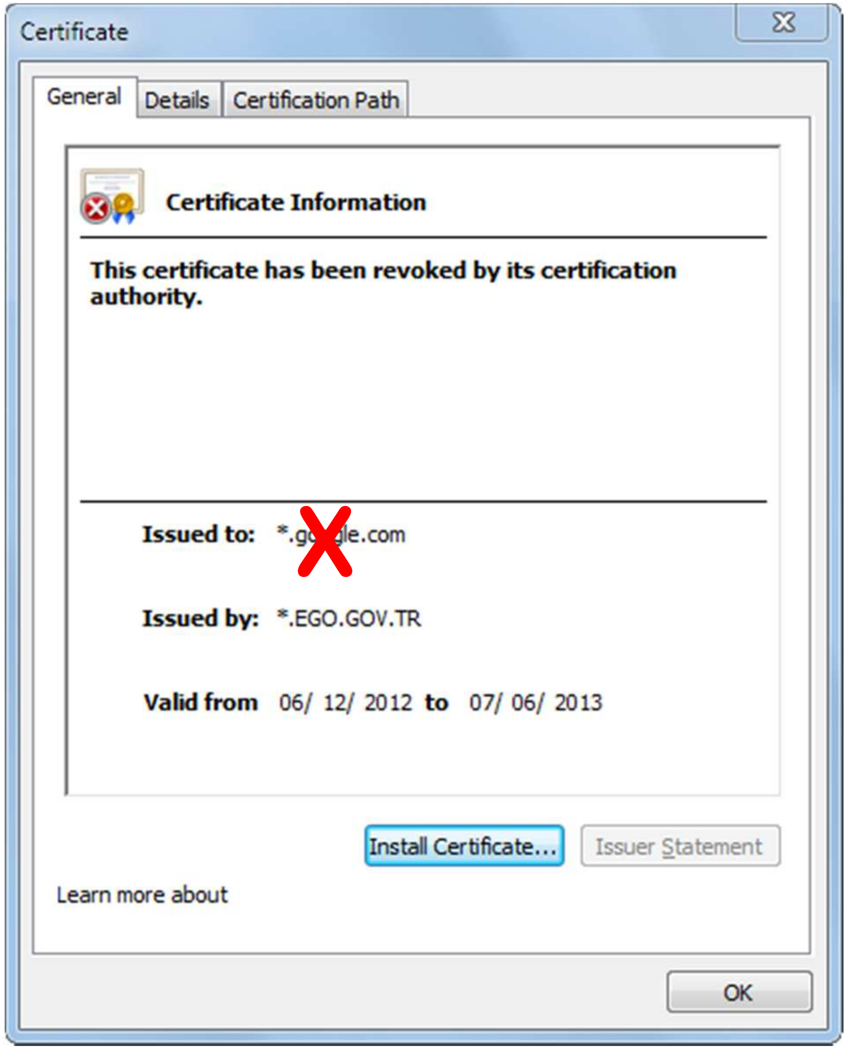
Show: <All>

Field	Value
Public key	RSA (1024 Bits)
Enhanced Key Usage	Server Authentication (1.3.6....
Subject Alternative Name	DNS Name=*.google.com, DN...
Basic Constraints	Subject Type=End Entity, Pat...
Thumbprint algorithm	sha1
Thumbprint	4d 85 47 b7 f8 64 13 2a 7f 62 ...
Extended Error Information	Revocation Status : The certifi...

```
DNS Name=*.google.com
DNS Name=*.android.com
DNS Name=*.appengine.google.com
DNS Name=*.cloud.google.com
DNS Name=*.google-analytics.com
DNS Name=*.google.ca
DNS Name=*.google.cl
DNS Name=*.google.co.in
DNS Name=*.google.co.jp
```

Learn more about certificate details

Examples



Certificate Information

This certificate has been revoked by its certification authority.

Issued to: *.google.com

Issued by: *.EGO.GOV.TR

Valid from 06/ 12/ 2012 **to** 07/ 06/ 2013

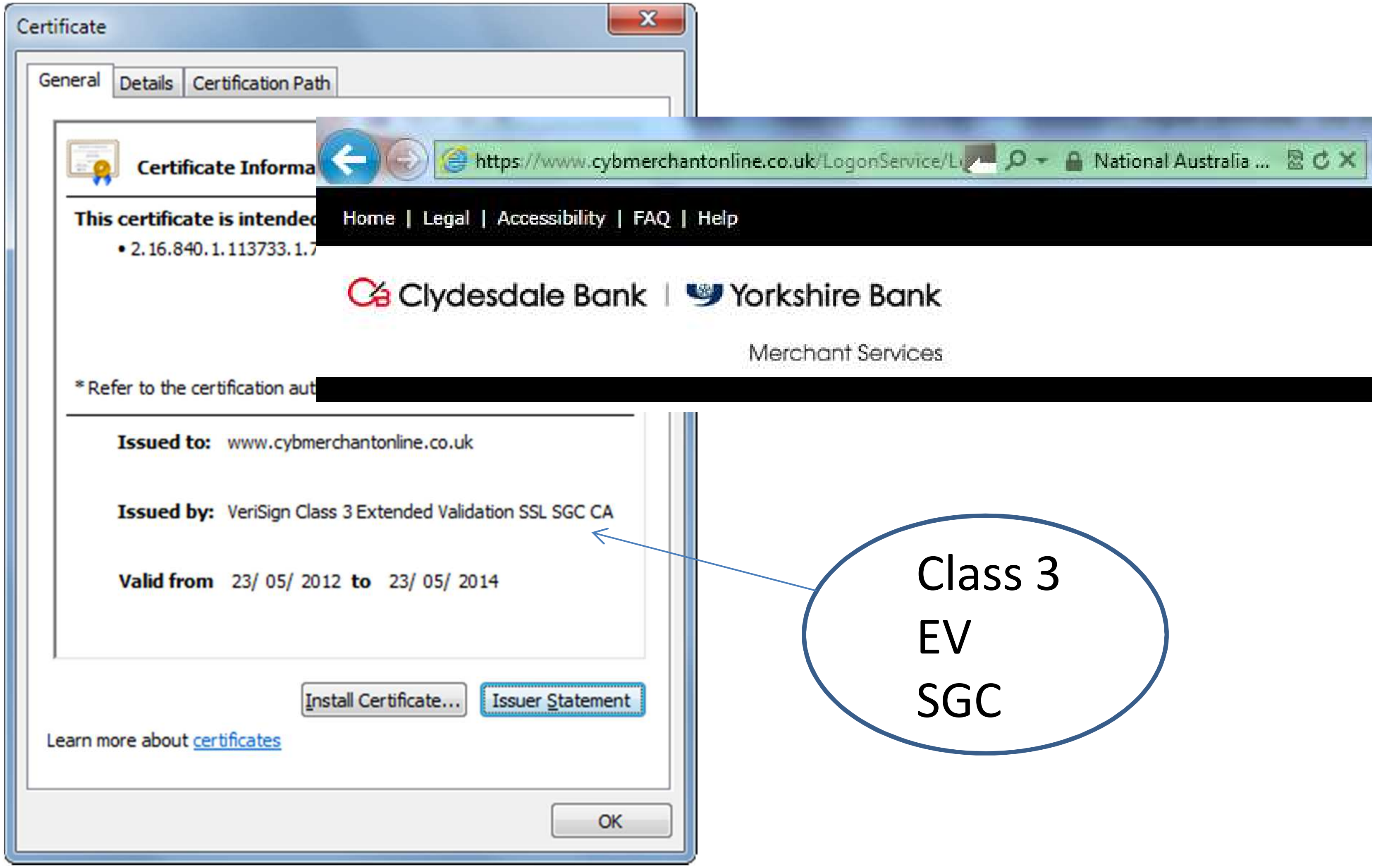
It's worth mentioning that when the ***certificate*** has a subject alternative domain name specified, as in this example, the ***browser*** doesn't check the Subject's Common Name.

www.ietf.org/rfc/rfc2818.txt

subjectAltName

```
DNS Name=*.google.com
DNS Name=*.android.com
DNS Name=*.appengine.google.com
DNS Name=*.cloud.google.com
DNS Name=*.google-analytics.com
DNS Name=*.google.ca
DNS Name=*.google.cl
DNS Name=*.google.co.in
DNS Name=*.google.co.jp
DNS Name=*.google.co.uk
DNS Name=*.google.com.ar
DNS Name=*.google.com.au
DNS Name=*.google.com.br
DNS Name=*.google.com.co
DNS Name=*.google.com.mx
DNS Name=*.google.com.tr
DNS Name=*.google.com.vn
DNS Name=*.google.de
DNS Name=*.google.es
DNS Name=*.google.fr
DNS Name=*.google.hu
DNS Name=*.google.it
DNS Name=*.google.nl
DNS Name=*.google.pl
DNS Name=*.google.pt
DNS Name=*.googleapis.cn
DNS Name=*.googlecommerce.com
DNS Name=*.gstatic.com
DNS Name=*.urchin.com
DNS Name=*.url.google.com
DNS Name=*.youtube-nocookie.com
DNS Name=*.youtube.com
DNS Name=*.ytimg.com
DNS Name=android.com
DNS Name=g.co
DNS Name=goo.gl
DNS Name=google-analytics.com
DNS Name=google.com
DNS Name=googlecommerce.com
DNS Name=urchin.com
DNS Name=youtu.be
DNS Name=youtube.com
```

Examples



https://www.cybmerchantonline.co.uk/LogonService/L

National Australia ...

Certificate Informa

This certificate is intende

- 2.16.840.1.113733.1.7

* Refer to the certification aut

Issued to: www.cybmerchantonline.co.uk

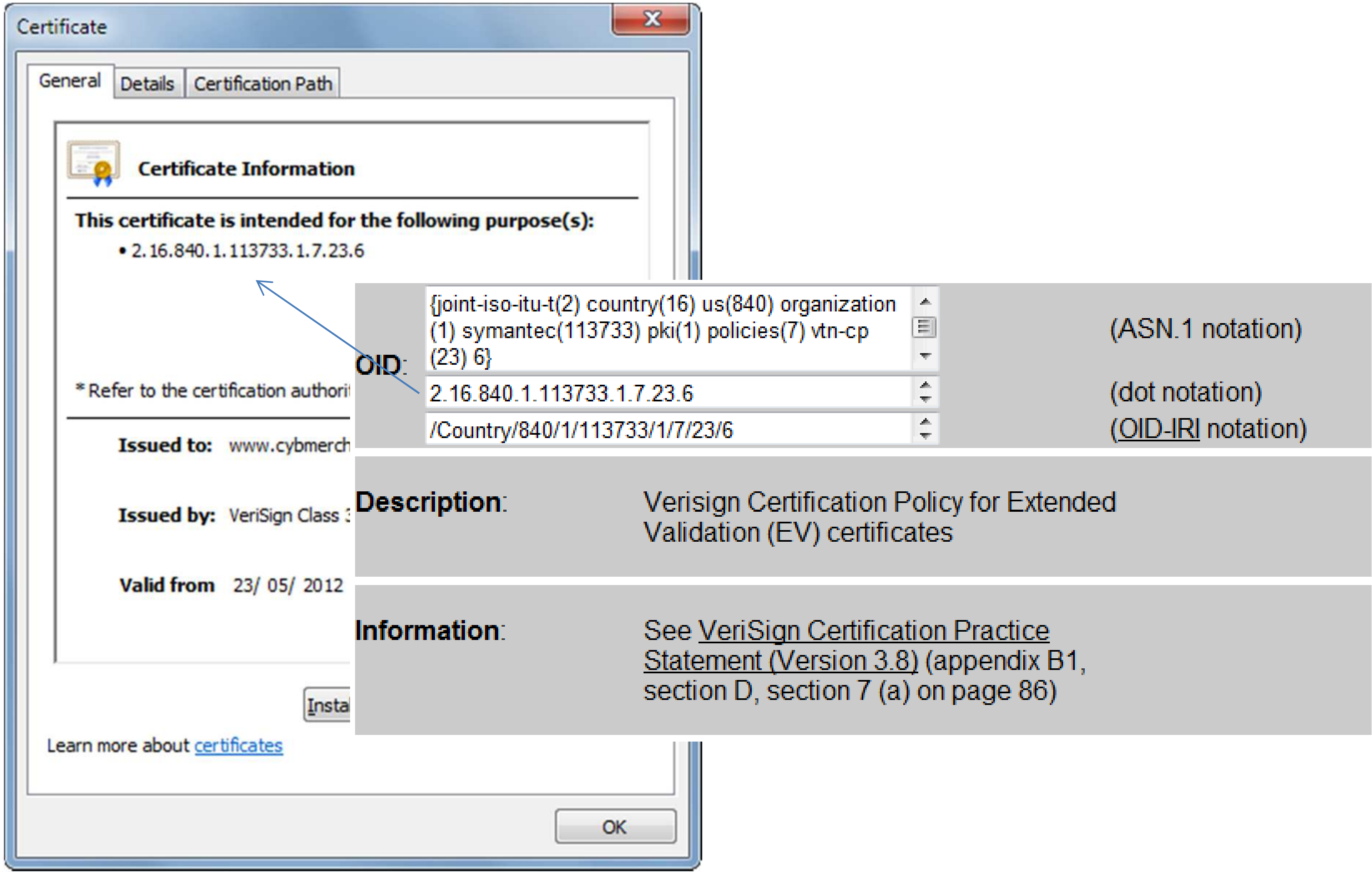
Issued by: VeriSign Class 3 Extended Validation SSL SGC CA

Valid from 23/ 05/ 2012 **to** 23/ 05/ 2014

Learn more about certificates

Class 3
EV
SGC

Examples



Certificate Information

This certificate is intended for the following purpose(s):

- 2.16.840.1.113733.1.7.23.6

* Refer to the certification authori

Issued to: www.cybmerch

Issued by: VeriSign Class 3

Valid from 23/ 05/ 2012

Learn more about certificates

OID:

{joint-iso-itu-t(2) country(16) us(840) organization (1) symantec(113733) pki(1) policies(7) vtn-cp (23) 6} (ASN.1 notation)

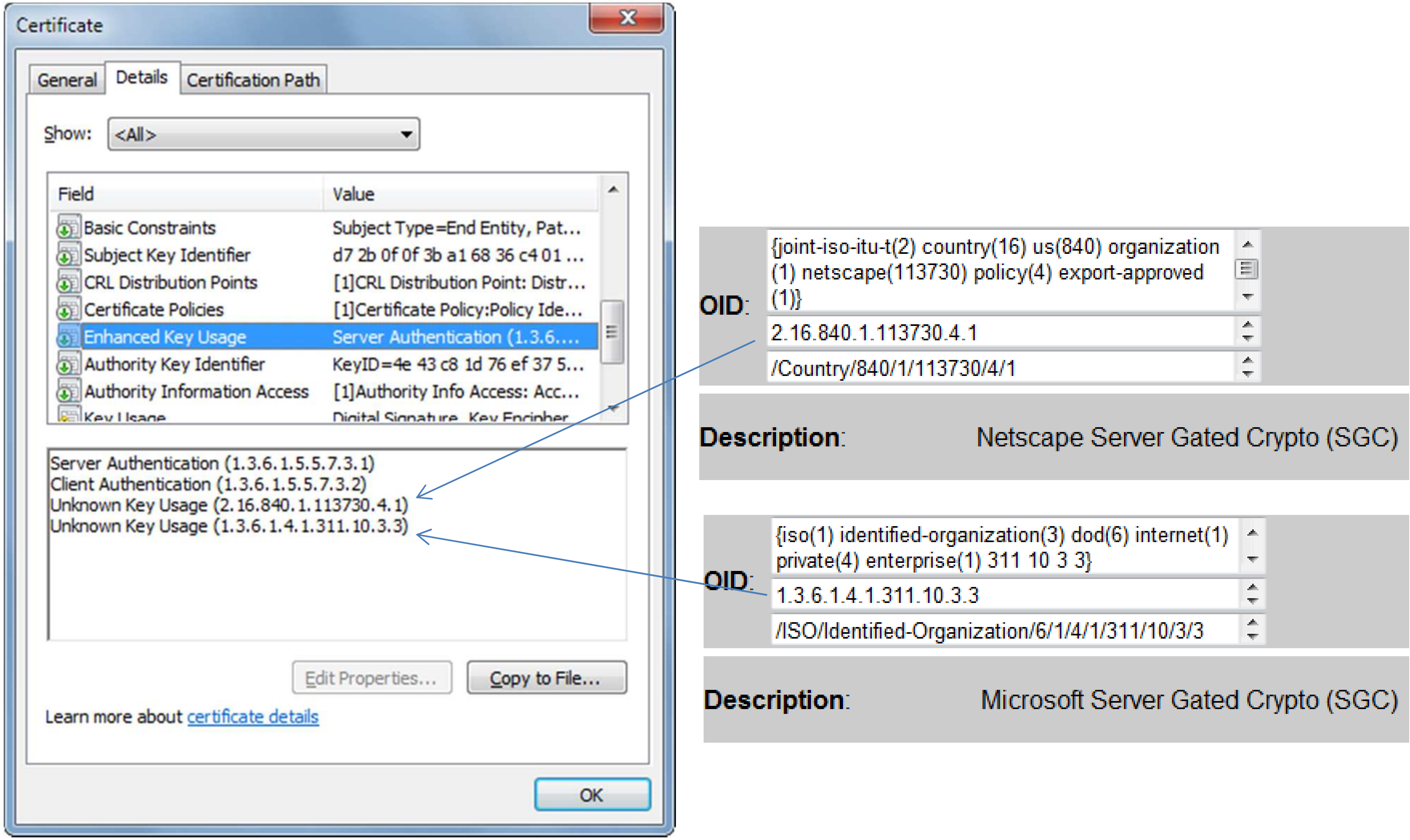
2.16.840.1.113733.1.7.23.6 (dot notation)

/Country/840/1/113733/1/7/23/6 (OID-IRI notation)

Description: Verisign Certification Policy for Extended Validation (EV) certificates

Information: See VeriSign Certification Practice Statement (Version 3.8) (appendix B1, section D, section 7 (a) on page 86)

Examples



Certificate

Show: <All>

Field	Value
Basic Constraints	Subject Type=End Entity, Pat...
Subject Key Identifier	d7 2b 0f 0f 3b a1 68 36 c4 01 ...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Enhanced Key Usage	Server Authentication (1.3.6....
Authority Key Identifier	KeyID=4e 43 c8 1d 76 ef 37 5...
Authority Information Access	[1]Authority Info Access: Acc...
Key Usage	Digital Signature, Key Encipher

```
Server Authentication (1.3.6.1.5.5.7.3.1)
Client Authentication (1.3.6.1.5.5.7.3.2)
Unknown Key Usage (2.16.840.1.113730.4.1)
Unknown Key Usage (1.3.6.1.4.1.311.10.3.3)
```

Learn more about certificate details

OID: {joint-iso-itu-t(2) country(16) us(840) organization (1) netscape(113730) policy(4) export-approved (1)}
2.16.840.1.113730.4.1
/Country/840/1/113730/4/1

Description: Netscape Server Gated Crypto (SGC)

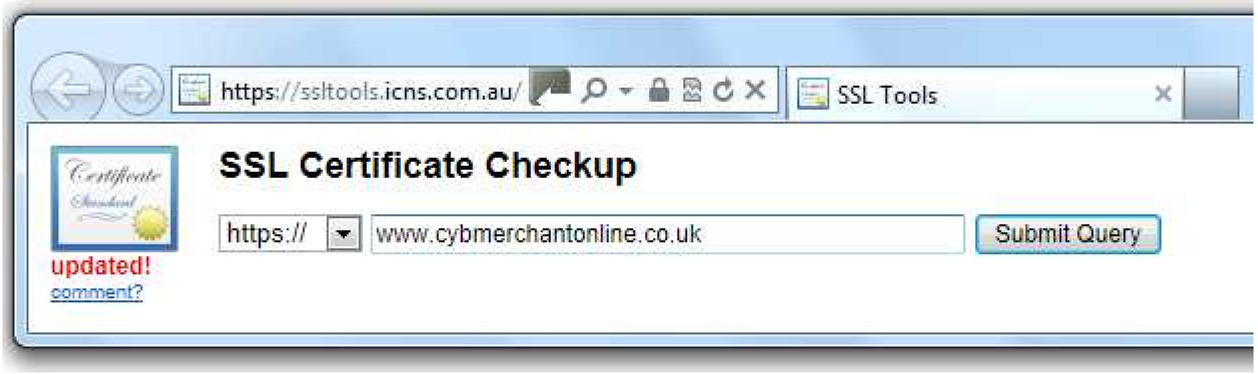
OID: {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) 311 10 3 3}
1.3.6.1.4.1.311.10.3.3
/ISO/Identified-Organization/6/1/4/1/311/10/3/3

Description: Microsoft Server Gated Crypto (SGC)

Examples

Really useful online certificate tools

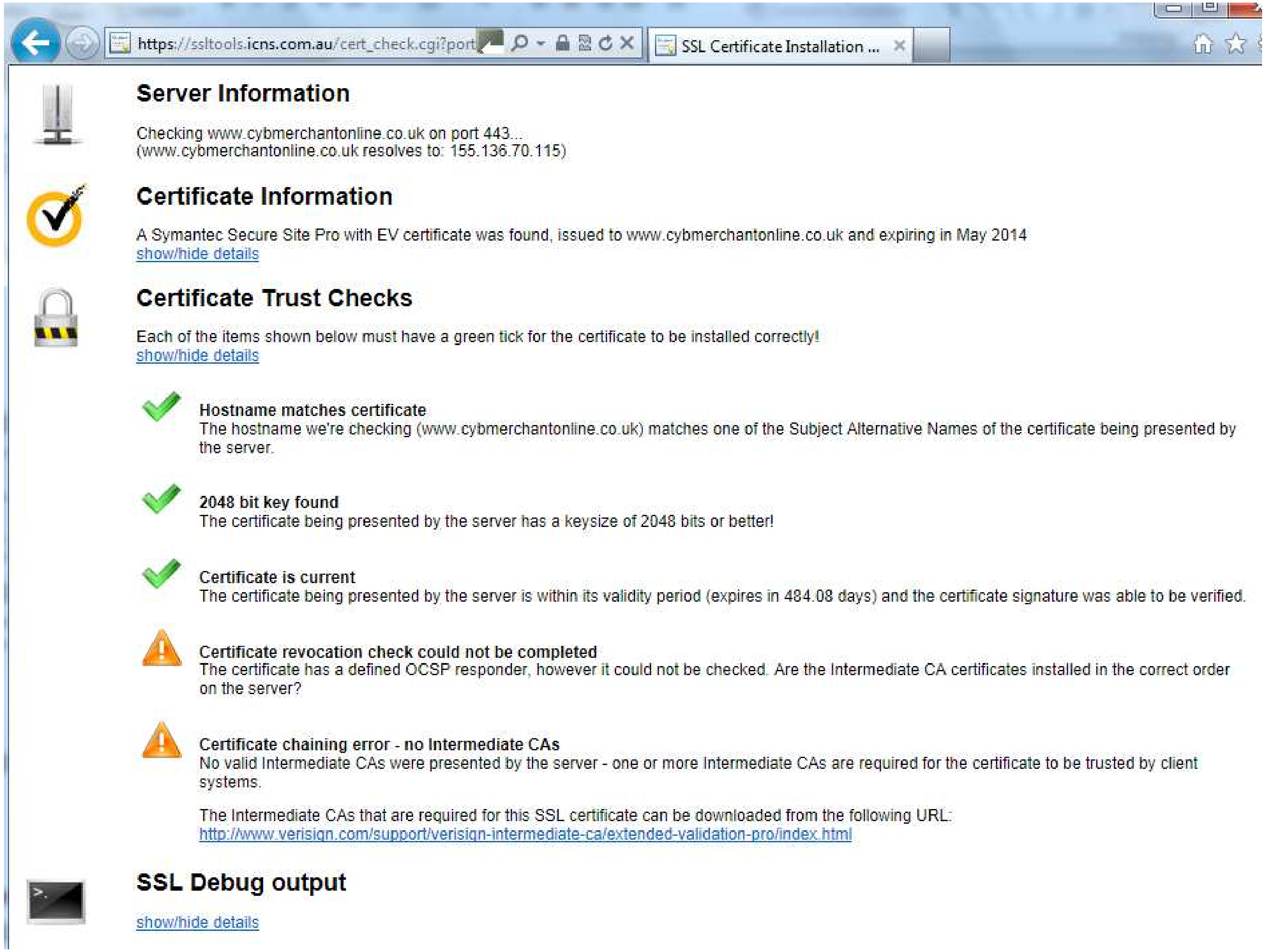
https://ssltools.icns.com.au/



SSL Certificate Checkup

https:// ▾ www.cybmerchantonline.co.uk

Examples



https://ssltools.icns.com.au/cert_check.cgi?port
SSL Certificate Installation ...

Server Information

Checking www.cybmerchantonline.co.uk on port 443...
(www.cybmerchantonline.co.uk resolves to: 155.136.70.115)

Certificate Information

A Symantec Secure Site Pro with EV certificate was found, issued to www.cybmerchantonline.co.uk and expiring in May 2014
show/hide details

Certificate Trust Checks

Each of the items shown below must have a green tick for the certificate to be installed correctly!
show/hide details

✓ **Hostname matches certificate**
The hostname we're checking (www.cybmerchantonline.co.uk) matches one of the Subject Alternative Names of the certificate being presented by the server.

✓ **2048 bit key found**
The certificate being presented by the server has a keysize of 2048 bits or better!

✓ **Certificate is current**
The certificate being presented by the server is within its validity period (expires in 484.08 days) and the certificate signature was able to be verified.

⚠ **Certificate revocation check could not be completed**
The certificate has a defined OCSP responder, however it could not be checked. Are the Intermediate CA certificates installed in the correct order on the server?

⚠ **Certificate chaining error - no Intermediate CAs**
No valid Intermediate CAs were presented by the server - one or more Intermediate CAs are required for the certificate to be trusted by client systems.

The Intermediate CAs that are required for this SSL certificate can be downloaded from the following URL:
http://www.verisign.com/support/verisign-intermediate-ca/extended-validation-pro/index.html

SSL Debug output

show/hide details

How are they managed with RACF

RACDCERT commands

ADD
GENREQ
GENCERT
LIST
EXPORT
DELETE

Certificate commands

CONNECT

tricky syntax !

ADDRING
LISTRING
DELRING

Keyring commands

SETROPTS REFRESH RACLIST(DIGTCERT,DIGTRING)

How are they managed with RACF

- RLIST DIGTCERT *
- RLIST DIGTRING *
- SR CLASS(DIGTCERT)
- SR CLASS(DIGTRING)
- RACDCERT ID(USER) LIST
- RACDCERT CERTAUTH LIST

Limited use as cannot be ‘filtered’

Problem solving techniques

- Make sure keyring looks correct !
- OpenSSL – especially for Server side SSL
  - https://ssltools.icns.com.au/ (online OpenSSL)
- Firefox – why and how
- Notepad++

OpenSSL

Sample commands:

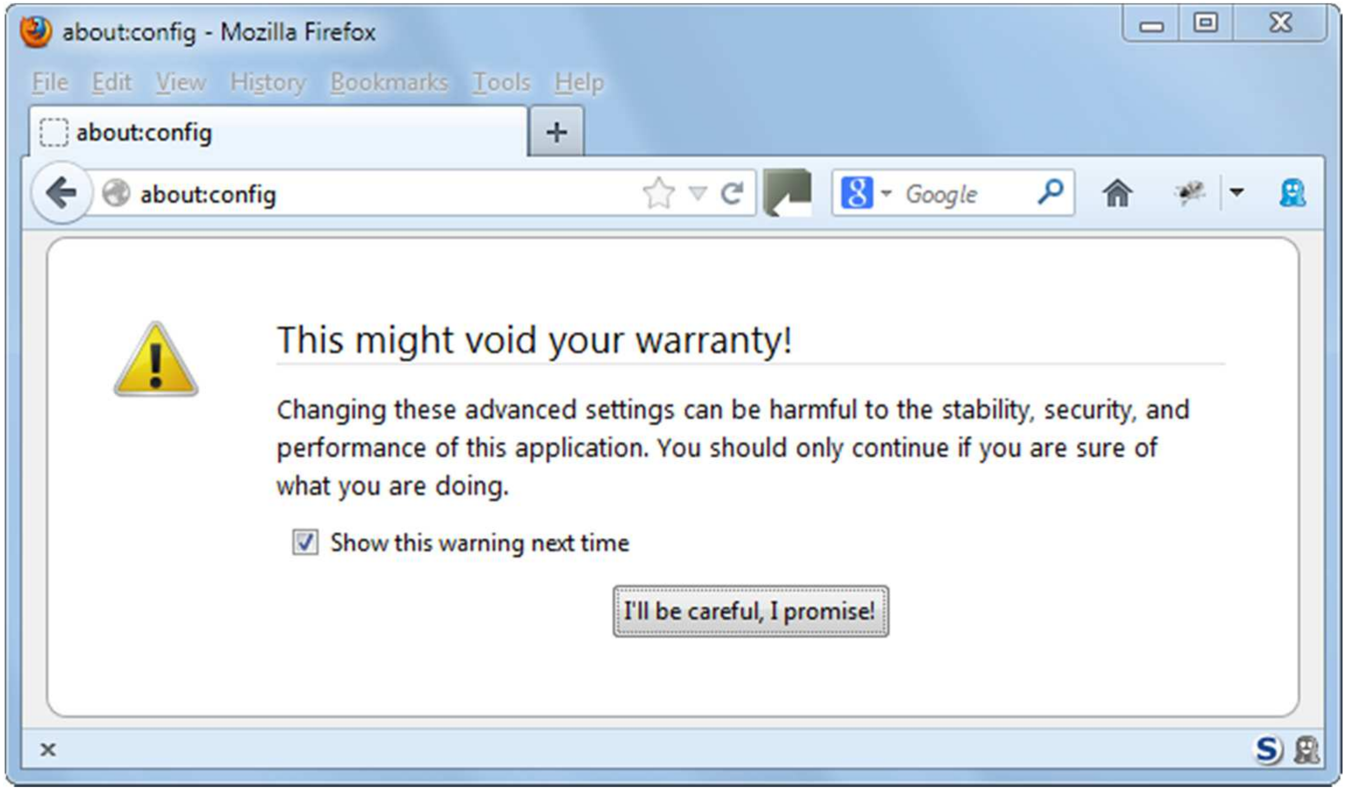
```
openssl.exe s_client -connect host:1414 -CAfile mq-roots.cer -state -verify 1 -tls1 -cipher NULL
openssl.exe s_client -connect host:1414 -CAfile mq-roots.cer -state -verify 1 -ssl3 -cipher NULL
openssl.exe s_client -connect host:1414 -CAfile mq-roots.cer -state -verify 1 -tls1

SSL-Session:
    Protocol  : TLSv1
    Cipher    : NULL-SHA

SSL-Session:
    Protocol  : SSLv3
    Cipher    : NULL-SHA

SSL-Session:
    Protocol  : TLSv1
    Cipher    : RC4-SHA
```

Firefox


about:config - Mozilla Firefox
File Edit View History Bookmarks Tools Help
about:config
about:config
Google

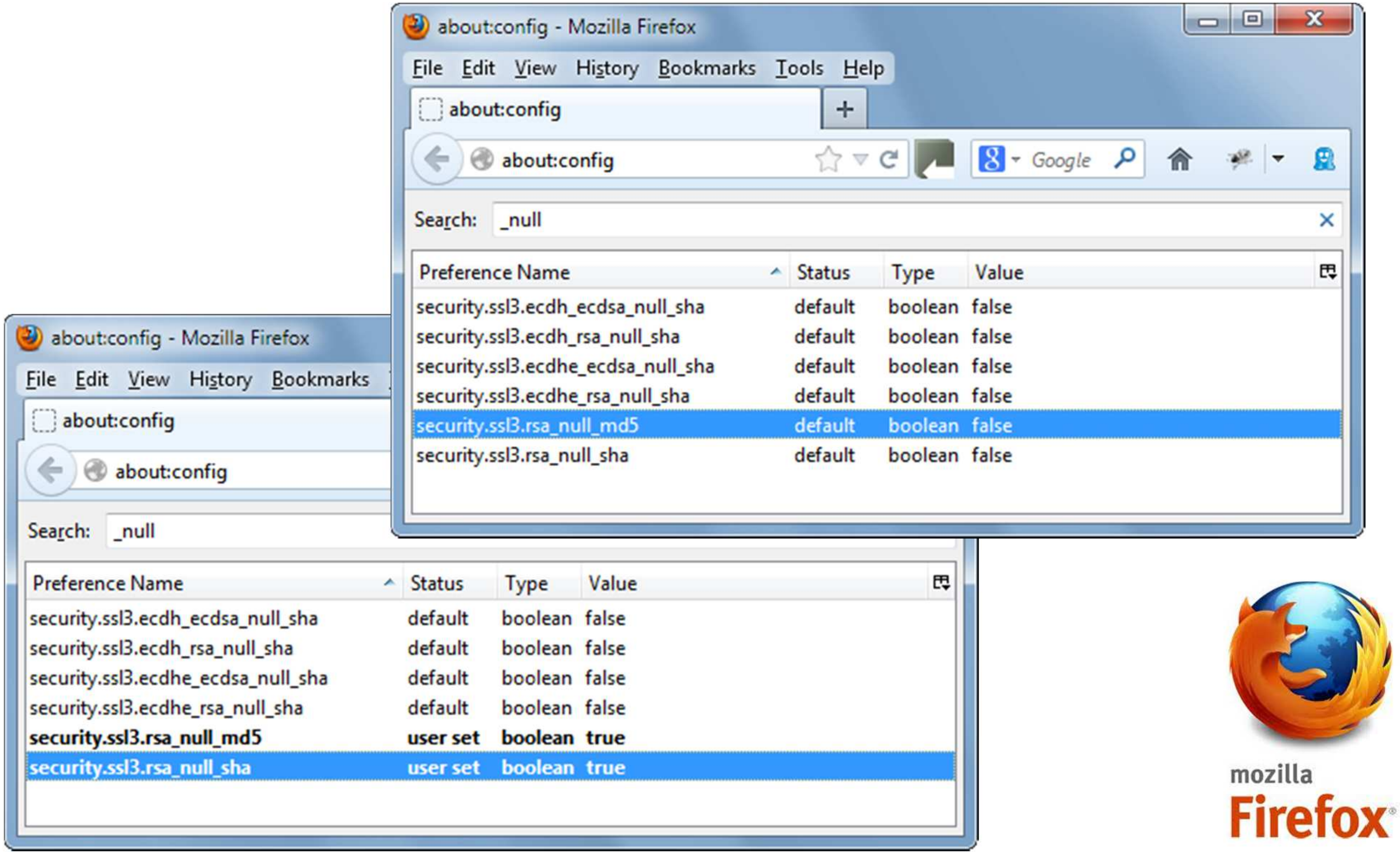
This might void your warranty!

Changing these advanced settings can be harmful to the stability, security, and performance of this application. You should only continue if you are sure of what you are doing.

☑ Show this warning next time

I'll be careful, I promise!

Firefox


about:config - Mozilla Firefox
File Edit View History Bookmarks Tools Help
about:config
Google

Search: _null

Preference Name	Status	Type	Value
security.ssl3.ecdh_ecdsa_null_sha	default	boolean	false
security.ssl3.ecdh_rsa_null_sha	default	boolean	false
security.ssl3.ecdhe_ecdsa_null_sha	default	boolean	false
security.ssl3.ecdhe_rsa_null_sha	default	boolean	false
security.ssl3.rsa_null_md5	default	boolean	false
security.ssl3.rsa_null_sha	default	boolean	false

about:config - Mozilla Firefox
File Edit View History Bookmarks
about:config

Search: _null

Preference Name	Status	Type	Value
security.ssl3.ecdh_ecdsa_null_sha	default	boolean	false
security.ssl3.ecdh_rsa_null_sha	default	boolean	false
security.ssl3.ecdhe_ecdsa_null_sha	default	boolean	false
security.ssl3.ecdhe_rsa_null_sha	default	boolean	false
security.ssl3.rsa_null_md5	**user set**	**boolean**	**true**
security.ssl3.rsa_null_sha	**user set**	**boolean**	**true**

Significance of NULL

SSL v3.0 cipher suites

SSL_RSA_WITH_NULL_MD5	NULL-MD5
SSL_RSA_WITH_NULL_SHA	NULL-SHA

SSL_RSA_EXPORT_WITH_RC4_40_MD5	EXP-RC4-MD5
SSL_RSA_WITH_DES_CBC_SHA	DES-CBC-SHA
SSL_RSA_WITH_RC4_128_MD5	RC4-MD5
SSL_RSA_WITH_RC4_128_SHA	RC4-SHA
SSL_RSA_WITH_IDEA_CBC_SHA	IDEA-CBC-SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA

http://www.openssl.org/docs/apps/ciphers.html#CIPHER_SUITE_NAMES

How to set-up for the purpose of encrypting 3270 sessions, SSL sessions

First thing, make sure you know what it should look like when done

```
READY
 RACDCERT ID(TCPIP) LISTRING(TNRING)

Digital ring information for user TCPIP:

  Ring:
       >TNRING<
  Certificate Label Name             Cert Owner     USAGE      DEFAULT
  --------------------------------   ------------   --------   -------
  ROOT                               CERTAUTH       CERTAUTH     NO

  TN3270                             ID(TCPIP)      PERSONAL     YES


READY
```

How to set-up for the purpose of encrypting 3270 sessions, SSL sessions

Generate new certificate

```
/*
 RACDCERT ID(TCPIP) +
  GENCERT +
  SUBJECTSDN(CN('common.name') + ←          Max length = 64
             OU('Organisational Unit') +
              O('Organisation') +
              L('Location') +
             SP('State Province') +
              C('Country')) +
  SIZE(2048) +
  NOTBEFORE(DATE(2013-02-06)) +
  NOTAFTER(DATE(2015-02-06)) +
  WITHLABEL('TN3270') + ←                   Max length = 32
  SIGNWITH(CERTAUTH LABEL('ROOT')) +
  KEYUSAGE(HANDSHAKE,DATAENCRYPT) +
  ALTNAME(EMAIL('geek@common.name') +
          URI('https://common.name') +
          DOMAIN('common.name') +
          IP(192.168.0.1))
/*
```

How to set-up for the purpose of encrypting 3270 sessions, SSL sessions

CONNECT example

```
/*
 RACDCERT +
  ID(TCPIP) +
  CONNECT(ID(TCPIP) +
  LABEL('TN3270') +
  RING(TNRING) +
  DEFAULT +
  USAGE(PERSONAL))
/*
 SETROPTS REFRESH RACLIST(DIGTCERT,DIGTRING)
/*
 RACDCERT ID(TCPIP) LIST(LABEL('TN3270'))
 RACDCERT ID(TCPIP) LISTRING(TNRING)
/*
```

Ring owner

Certificate owner

How to set-up for the purpose of encrypting 3270 sessions, SSL sessions

```
/*
 RACDCERT ID(TCPIP) +
          ADD('HLQ.TCPIP.NEW') +
          TRUST +
          WITHLABEL('TN3270') +
          PASSWORD('********')
/*
```

```
READY
 RACDCERT ID(USERID) ADD('HLQ.CERT') WITHLABEL('test import')
IRRD103I An error was encountered processing the specified input data set.
READY
```

ADD gotchas - input dataset must be allocated as VB in order to avoid

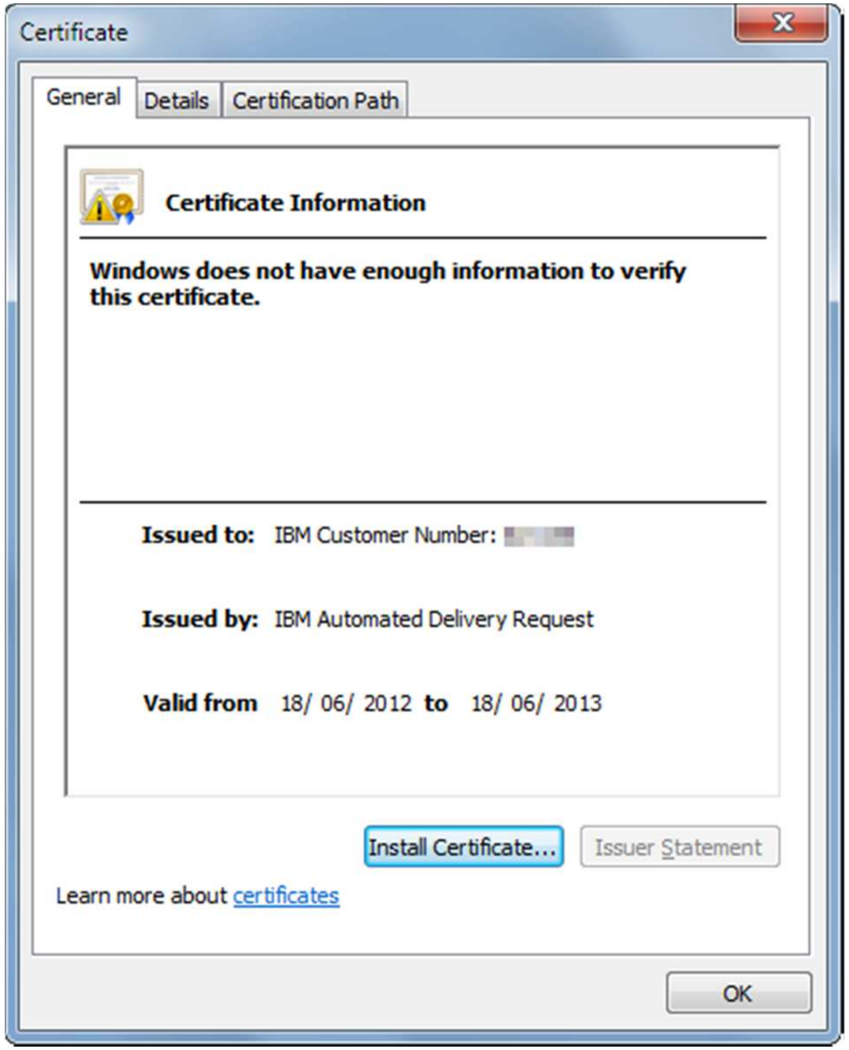
Base64 specification always has maximum line length.
If file has come from a Unix system and only has LF instead of CR/LF then
RACF will fail to process the data as max line length will have been exceeded.

More gotchas

- If ‘withlabel’ parameter is omitted from RACDCERT command, it defaults to:
  - LABEL000000001
  - LABEL000000002   etc.

- Certificates are ‘owned’ by ID – deleting the owning ID automatically deletes ALL certificates owned by that ID !

SMPE Example



Certificate

Certificate Information

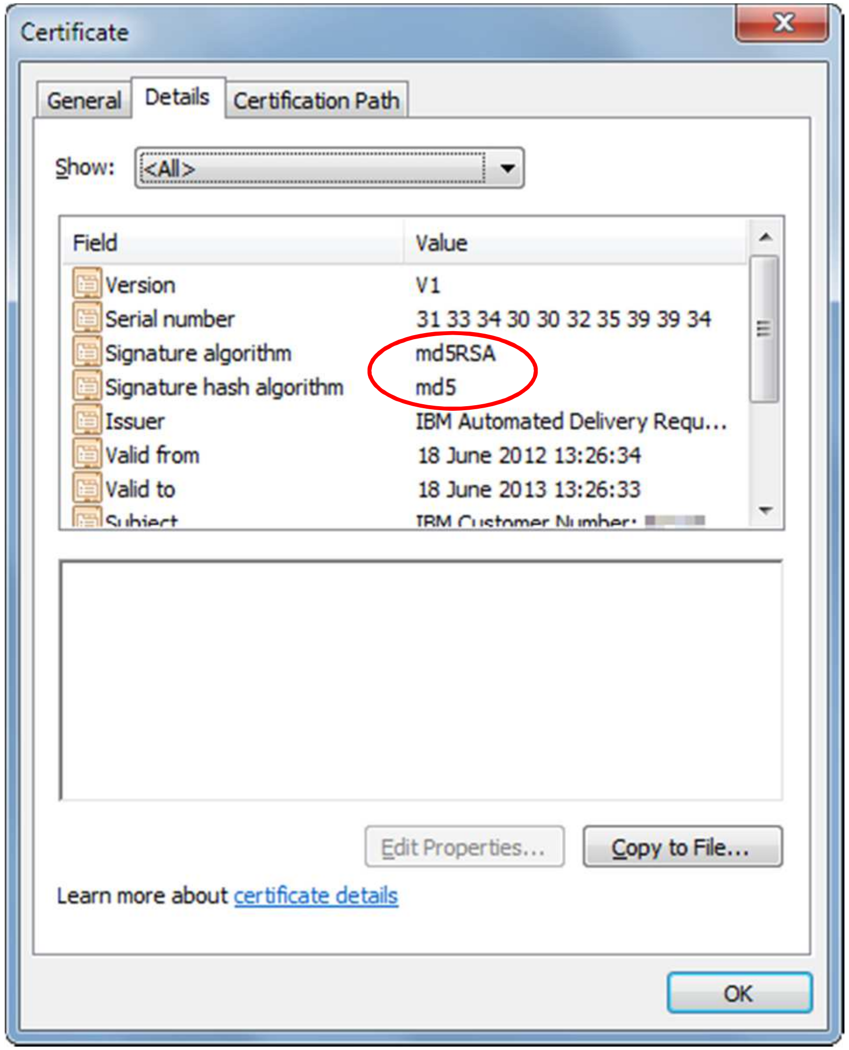
Windows does not have enough information to verify this certificate.

Issued to: IBM Customer Number: [redacted]

Issued by: IBM Automated Delivery Request

Valid from 18/ 06/ 2012 **to** 18/ 06/ 2013

Learn more about certificates



Certificate

Show: <All>

Field	Value
Version	V1
Serial number	31 33 34 30 30 32 35 39 39 34
Signature algorithm	md5RSA
Signature hash algorithm	md5
Issuer	IBM Automated Delivery Requ...
Valid from	18 June 2012 13:26:34
Valid to	18 June 2013 13:26:33
Subject	IBM Customer Number: [redacted]

Learn more about certificate details

SMPE Example

```
READY
 RACDCERT ID(******) LISTRING(SMPERING)

Digital ring information for user ******:

  Ring:
       >SMPERING<
  Certificate Label Name             Cert Owner     USAGE      DEFAULT
  --------------------------------   ------------   --------   -------
  Equifax Secure CA                  CERTAUTH       CERTAUTH     NO

  SMPE CLIENT CERT 2012              ID(******)     CERTAUTH     NO


READY
```

https://www14.software.ibm.com/webapp/ShopzSeries/ShopzSeries.jsp

Discuss code from racf.co.uk

- RACF119 List every certificate in RACF
- RACF133 Export every certificate in RACF
- **RACF109 Search for certificates in RACF**

RACF109 is a search engine like search which searches serial number, common name* certificate owner and certificate label.

* Remember RACF unload uses CN of issuer, not the actual CN of the certificate!

Tools

Base64	http://www.fourmilab.ch/webtools/base64/
Certmgr.msc	Microsoft Windows
DumpASN1	http://www.nigelpentland.co.uk/dumpasn1/
Firefox	http://www.mozilla.org/en-US/
Notepad++	http://notepad-plus-plus.org/
OpenSSL	http://slproweb.com/products/Win32OpenSSL.html
Portecle	http://portecle.sourceforge.net/
RACF PC Utilities	http://www.racf.co.uk/

Thank you!

National Australia Bank

GSE
GUIDE SHARE EUROPE
UK REGION

Digital Certificates

Principles of operation

Nigel Pentland

National Australia Group