

# Current TLS Certificate Profile

Thomas Hardjono

*VeriSign*

*thardjono@verisign.com*

# Current TLS Cert Profile

Subject DN

=====

CN = <FQDN of Server>

OU = Terms of use at [www.verisign.com/rpa](http://www.verisign.com/rpa) (c)00

OU = <Org Unit of Organization> OPTIONAL

O = <Full Organization Name>

L = <City>

S = <State/Province - no abbrevs>

C = <2 Letter ISO country code>

# Current TLS Cert Profile (cont)

Extensions

=====

basicConstraints :

Subject Type=End Entity

certificatePolicies :

PolicyIdentifier=2.16.840.1.113733.1.7.23.3

[1,1]Policy Qualifier Info:

Policy Qualifier Id=CPS

Qualifier:

<https://www.verisign.com/rpa>

keyUsage:

Digital Signature

Key Encipherment(A0)

extendedKeyUsage:

Server Authentication(1.3.6.1.5.5.7.3.1)

Client Authentication(1.3.6.1.5.5.7.3.2)

# Current TLS Cert Profile (cont)

authorityInformationAccess:

[1]Authority Info Access

Access Method=On-line Certificate Status

Protocol(1.3.6.1.5.5.7.48.1)

Alternative Name:

URL=http://ocsp.verisign.com

crlDistributionPoints:

[1]CRL Distribution Point

Distribution Point Name:

Full Name:

URL=http://crl.verisign.com/Class3InternationalServer.crl

# Example Certificate

Version	V3
Serial number	6100 59D8 6A81 04C5 3BF7 9E2B BDC8 62A1
Signature algorithm	md5RSA
Issuer	OU = www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign OU = VeriSign International Server CA - Class 3 OU = VeriSign, Inc. O = VeriSign Trust Network
Valid from	Sunday, September 29, 2002 7:00:00 PM
Valid to	Tuesday, September 30, 2003 6:59:59 PM
Subject	CN = developer.grandcentral.com OU = Terms of use at www.verisign.com/rpa (c)00 OU = developer site O = Grand Central Communications L = San Francisco S = California C = US
Public key	RSA (1024bits) 3081 8902 8181 00FC 9840 7299 A5AC 2AA4 26B1 B5D4 C0AB 0744 3256 53EE 7AEE 68EA 2940 A023 657B 5791 8DC2 15D4 9591 05B0 54D6 50AC B9E0 1D0F 27D9 24FC 7BFC CDAB 1C89 63F4 EFF6 7CED C1D5 E6EC A79B 60A5 B893 B5C7 08F6 2994 ECA1 9714 613F C705 5726 D3A6 C00F 00DD 8D36 36E7 FBAF 80B2 0F07 49C5 323C AEBA 92C6 51AD 746E 6FB6 66A7 1760 F850 4902 0301 0001
<b>Basic Constraints</b>	Subject Type=End Entity Path Length Constraint=None

# Example Certificate (cont.)

<b>Certificate Policies</b>	[1]Certificate Policy: PolicyIdentifier=2.16.840.1.113733.1.7.23.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.verisign.com/rpa
<b>Key Usage</b>	Digital Signature , Key Encipherment(A0)
<b>Enhanced Key Usage</b>	Unknown Key Usage(2.16.840.1.113730.4.1) Server Authentication(1.3.6.1.5.5.7.3.1) Client Authentication(1.3.6.1.5.5.7.3.2)
<b>Authority Information Access</b>	[1]Authority Info Access Access Method=On-line Certificate Status Protocol(1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.verisign.com
<b>CRL Distribution Points</b>	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.verisign.com/Class3InternationalServer.crl
<b>2.16.840.1.113733.1.6.15</b> (nb. Dun & Bradstreet OID)	16 09 38 38 34 32 34 34 ..884244 30 35 39 059
Thumbprint algorithm	sha1
Thumbprint	3042 5577 25A3 F15B 31A2 EE84 E4C1 1117 0B92 B250

END  
+  
Thank You