



TECHNICAL BULLETIN

Software 4.0.7 | November 2014 | 3725-49116-001

Certificate Updates For Polycom[®] UC Software 4.0.7

For SoundPoint[®] IP, SoundStation[®] IP, SoundStation Duo[™], and VVX[®] Phones

Copyright © 2014, Polycom, Inc. All rights reserved. No part of this document may be reproduced, translated into another language or format, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc.

6001 America Center Drive
San Jose, CA 95002
USA



Polycom®, the Polycom logo and the names and marks associated with Polycom products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

End User License Agreement By installing, copying, or otherwise using this product, you acknowledge that you have read, understand and agree to be bound by the terms and conditions of the [End User License Agreement](#) for this product.

Patent Information The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

Open Source Software Used in this Product This product may contain open source software. You may receive the open source software from Polycom up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to Polycom of shipping or distributing the software to you. To receive software information, as well as the open source software code used in this product, contact Polycom by email at OpenSourceVideo@polycom.com.

Disclaimer While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

Limitation of Liability Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.

Customer Feedback We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocumentationFeedback@polycom.com.



Visit the [Polycom Support Center](#) for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.

Contents

Certificate Updates For Polycom UC Software 4.0.7	4
<i>Customer Impact</i>	<i>4</i>
Unsupported Thawte MD5 Based Root Certificates.....	4
<i>Thawte Personal Basic CA-md5WithRSA</i>	<i>4</i>
<i>Thawte Personal Freemail CA-md5WithRSA</i>	<i>6</i>
<i>Thawte Personal Premium CA-md5WithRSA.....</i>	<i>8</i>
<i>Thawte Premium Server CA-md5WithRSA.....</i>	<i>11</i>
<i>Thawte Server CA-md5WithRSA.....</i>	<i>13</i>
Supported Thawte SHA1 Based Root Certificates	16
<i>Thawte Personal Basic CA-sha1WithRSA.....</i>	<i>16</i>
<i>Thawte Personal Freemail CA-sha1WithRSA.....</i>	<i>18</i>
<i>Thawte Personal Premium CA-sha1WithRSA</i>	<i>20</i>
<i>Thawte Premium Server CA-sha1WithRSA.....</i>	<i>22</i>
<i>Thawte Server CA-sha1WithRSA.....</i>	<i>24</i>

Certificate Updates For Polycom UC Software 4.0.7

Polycom now supports the SHA1 Thawte certificates and no longer supports the Thawte MD5 certificates.

Customer Impact

If you are using the Thawte MD5 CA issued certificates, Polycom recommends that you migrate to SHA1-based secure certificates. If you continue to use Thawte MD5 CA signed certificates, the secure communication with the device can fail. Both the unsupported and supported certificates are listed below.

No Longer Supported Thawte MD5 Based Root Certificates

- [Thawte Personal Basic CA-md5WithRSA](#)
- [Thawte Personal Freemail CA-md5WithRSA](#)
- [Thawte Personal Premium CA-md5WithRSA](#)
- [Thawte Premium Server CA-md5WithRSA](#)
- [Thawte Server CA-md5WithRSA](#)

Thawte Personal Basic CA-md5WithRSA

=====

MD5 Fingerprint: E6:0B:D2:C9:CA:2D:88:DB:1A:71:0E:4B:78:EB:02:41

PEM Data:

-----BEGIN CERTIFICATE-----

```
MIIDITCCAoqgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBYzELMAkGA1UEBhMCWkEx
FTATBgNVBAGTDGFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMjQ2FwZSBUB3duMR0wGAYD
VQQKEGFUaGF3dGUgQ29uc3VsdGluZzEoMCMYGA1UECXMfQ2VydGlmaWNhdGlvbiBT
ZXJ2aWNlcyBEaXZpc2lvbjEhMB8GA1UEAxMYVGhhZD3RIIFBlcnNvbmlhcnJlc2l
IENBMSgwJgYJKoZIhvcNAQkBFHlwZXJ2b25hbC1iYXNpY0B0aGF3dGUuY29tMB4X
DTk2MDEwMTAwMDAwMFMoXDTIwMTIzMTIzNTk1OVowgcxkZAJBgNVBAYTAipBMRUw
```

```
EwYDVQIQIExwXZXXN0ZXJulENhcGUxEjAQBgNVBAcTCUNhcGUgVG93bjEaMBGGA1UE
ChMRVGHhd3RIIENvbnN1bHRpbmcxKDAmBgNVBAcTH0NlcnRpZmljYXRpb24gU2Vy
dmljZXMgRGI2aXNpb24xITAFBgNVBAMTGFRoYXd0ZSBQZXJzb25hbCBCYXNpYyBD
QTEoMCMYGCsqGSIb3DQEJARYZcGVyc29uYWwtYmFzaWNAdGhhd3RlLmNvbTcBnzAN
BkgqhkiG9w0BAQEFAAOBJQAwgYkCgYEAvLyTU23AUE+CFeZIIDWmWr5vQvoPR+53
dXLdjUmbllgeNTPK1GzaQuRdhciB5dqxFGTS+CN7zeVoQxN2jSQHReJl+A1OFdK
wPQlCok8RHtQfmGakOMj04gRRif1CwcOu93RfyAKiLIWCy4cgNrx454p7xS9CkT7
G1sY0b8jkyECAwEAAaMTMBEwDwYDVR0TAQH/BAUwAwEB/zANBgqhkiG9w0BAQQF
AAOBGQAt4plrsD16iddZopQBHyvdEktTwq1/qqcAXJFAVYVKOKqEcLnZgA+le1z7
c8a914pHXAPJLSeoF+CEhULcXpvGt7Jtu3Sv5D/Lp7ew4F2+eIMIINLbgQ95B21P
9DKVWIIBe94y1k049hJcBIDfBVu9FEuh3ym6O0GN92NWod8isQ==
```

-----END CERTIFICATE-----

Certificate Ingredients:

Data:

Version: 3 (0x2)

Serial Number: 0 (0x0)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting, OU=Certification Services Division, CN=Thawte Personal Basic CA/Email=personal-basic@thawte.com

Validity

Not Before: Jan 1 00:00:00 1996 GMT

Not After : Dec 31 23:59:59 2020 GMT

Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting, OU=Certification Services Division, CN=Thawte Personal Basic CA/Email=personal-basic@thawte.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:bc:bc:93:53:6d:c0:50:4f:82:15:e6:48:94:35:

a6:5a:be:6f:42:fa:0f:47:ee:77:75:72:dd:8d:49:

9b:96:57:a0:78:d4:ca:3f:51:b3:69:0b:91:76:17:
 22:07:97:6a:c4:51:93:4b:e0:8d:ef:37:95:a1:0c:
 4d:da:34:90:1d:17:89:97:e0:35:38:57:4a:c0:f4:
 08:70:e9:3c:44:7b:50:7e:61:9a:90:e3:23:d3:88:
 11:46:27:f5:0b:07:0e:bb:dd:d1:7f:20:0a:88:b9:
 56:0b:2e:1c:80:da:f1:e3:9e:29:ef:14:bd:0a:44:
 fb:1b:5b:18:d1:bf:23:93:21

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

Signature Algorithm: md5WithRSAEncryption

2d:e2:99:6b:b0:3d:7a:89:d7:59:a2:94:01:1f:2b:dd:12:4b:
 53:c2:ad:7f:aa:a7:00:5c:91:40:57:25:4a:38:aa:84:70:b9:
 d9:80:0f:a5:7b:5c:fb:73:c6:bd:d7:8a:61:5c:03:e3:2d:27:
 a8:17:e0:84:85:42:dc:5e:9b:c6:b7:b2:6d:bb:74:af:e4:3f:
 cb:a7:b7:b0:e0:5d:be:78:83:25:94:d2:db:81:0f:79:07:6d:
 4f:f4:39:15:5a:52:01:7b:de:32:d6:4d:38:f6:12:5c:06:50:
 df:05:5b:bd:14:4b:a1:df:29:ba:3b:41:8d:f7:63:56:a1:df:
 22:b1

Thawte Personal Freemail CA-md5WithRSA

=====

MD5 Fingerprint: 1E:74:C3:86:3C:0C:35:C5:3E:C2:7F:EF:3C:AA:3C:D9

PEM Data:

-----BEGIN CERTIFICATE-----

MIIDLTCcApagAwIBAgIBADANBgkqhkiG9w0BAQQFADCB0TElMAkGA1UEBhMCWkEx
 FTATBgNVBAGTDfDlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBUb3duMR0wGAYD
 VQKExFUaGF3dGUgQ29uc3VsdGluZzEoMCYGA1UECxMfQ2VydGlmaWNhdGlubiBT

ZXJ2aWNlcyBEaXZpc2lvdjEkmCIGA1UEAxMbvGhhd3RlIFBlcnNvbmcFslEzYzZWVt
 YWlsIENBMSswKQYJKoZIhvcNAQkBFhwwZXJzb25hbC1mcmVlbWVpEBoaGF3dGUu
 Y29tMB4XDk2MDEwMTAwMDAwMFoXDTEwMTIzMTIzNTk1OVowgdExCzAJBgNVBAYT
 AlpBMRUwEwYDVQQIEwxxZXN0ZXJlIENhcGUxEjAQBgNVBAcTCUNhcGUgVG93bjEa
 MBgGA1UEChMRVGVhd3RlIENvbnN1bHRpbmcxKDAmbGVBAsTH0NlcnRpZmljYXRp
 b24gU2VydmljZXMGRI2aXNpb24xJDAiBgNVBAMTG1RoYXd0ZSBQZXJzb25hbCBG
 cmVlbWVpEBoaCBQDQTErMCKGCSqGSIb3DQEJARYccGVyc29uYWwtZnJlZW1haWxAdGhh
 d3RlImNvbTCBnzANBkgqhkiG9w0BAQEFAAOBjQAwgYkCgYEA1GnX1LCUZftx6UfY
 DFG26nKRslRefSONj3sS34UldSh0OkIsYeflXtL734Zhx2G6qPduc6WZBrCFG5E
 rHzmj+hND3EfQDimAKOHePb5IIZererAXnbr2RSjXW56fAylS1V/Bhkp56aJtVq
 uzgkCGqYx7Hao5iR/Xnb5VrEHLkCAwEAAaMTMBEwDwYDVR0TAQH/BAUwAwEB/zAN
 BgkqhkiG9w0BAQQFAAOBqQDH7JJ+TvjlIqVnYiqk8E0RYNBvjWBYyawmu1I1XAjP
 MPuoSpaKH2JCI4wXD/S6ZJwXrEcp352YXtJsYHFcoqzceePnbgBHH7UNKOgCneSa
 /RPOptl8sfjcXyMmCZGAc9AUG95DqYMI8uacLxXK/qarigd1iwzdUYRr5PjRznei
 gQ==

-----END CERTIFICATE-----

Certificate Ingredients:

Data:

Version: 3 (0x2)

Serial Number: 0 (0x0)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting, OU=Certification Services Division, CN=Thawte Personal Freemail CA/Email=personal-freemail@thawte.com

Validity

Not Before: Jan 1 00:00:00 1996 GMT

Not After : Dec 31 23:59:59 2020 GMT

Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting, OU=Certification Services Division, CN=Thawte Personal Freemail CA/Email=personal-freemail@thawte.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:d4:69:d7:d4:b0:94:64:5b:71:e9:47:d8:0c:51:
b6:ea:72:91:b0:84:5e:7d:2d:0d:8f:7b:12:df:85:
25:75:28:74:3a:42:2c:63:27:9f:95:7b:4b:ef:7e:
19:87:1d:86:ea:a3:dd:b9:ce:96:64:1a:c2:14:6e:
44:ac:7c:e6:8f:e8:4d:0f:71:1f:40:38:a6:00:a3:
87:78:f6:f9:94:86:5e:ad:ea:c0:5e:76:eb:d9:14:
a3:5d:6e:7a:7c:0c:a5:4b:55:7f:06:19:29:7f:9e:
9a:26:d5:6a:bb:38:24:08:6a:98:c7:b1:da:a3:98:
91:fd:79:db:e5:5a:c4:1c:b9

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

Signature Algorithm: md5WithRSAEncryption

c7:ec:92:7e:4e:f8:f5:96:a5:67:62:2a:a4:f0:4d:11:60:d0:
6f:8d:60:58:61:ac:26:bb:52:35:5c:08:cf:30:fb:a8:4a:96:
8a:1f:62:42:23:8c:17:0f:f4:ba:64:9c:17:ac:47:29:df:9d:
98:5e:d2:6c:60:71:5c:a2:ac:dc:79:e3:e7:6e:00:47:1f:b5:
0d:28:e8:02:9d:e4:9a:fd:13:f4:a6:d9:7c:b1:f8:dc:5f:23:
26:09:91:80:73:d0:14:1b:de:43:a9:83:25:f2:e6:9c:2f:15:
ca:fe:a6:ab:8a:07:75:8b:0c:dd:51:84:6b:e4:f8:d1:ce:77:
a2:81

Thawte Personal Premium CA-md5WithRSA

=====

MD5 Fingerprint: 3A:B2:DE:22:9A:20:93:49:F9:ED:C8:D2:8A:E7:68:0D

PEM Data:

-----BEGIN CERTIFICATE-----

MIIDKCCApKgAwIBAgIBADANBgkqhkiG9w0BAQQFADCzELMAkGA1UEBhMCWkEx
FTATBgNVBAGTDfDlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBUb3duMRRowGAYD
VQKExFUaGF3dGUgQ29uc3VsdGluZzEoMCYGA1UECXMfQ2VydGlmaWNhdGlvbIbT
ZXJ2aWNlcyBEaXZpc2lvbEjMCEGA1UEAxMaVGhhd3RlIFBlcnNvbmsFsIFByZW1p
dW0gQ0ExKjAoBgkqhkiG9w0BCQEWG3BlcnNvbmsLXByZW1pdW1AdGhhd3RlLmNv
bTAeFw05NjAxMDEwMDAwMDBaFw0yMDEyMzEyMzU5NTlaMIIHMQswCQYDVQGEwJa
QTEVMBMGA1UECBMMV2VzdGVybiBDYXBIMRlwEAYDVQQHEwIDYXBIIFRvd24xGjAY
BgNVBAoTEVRoYXZ0ZSBDd25zdWx0aW5nMSgwJgYDVQQLEx9DZXJ0aWZpY2F0aW9u
IFNlcnZpY2VzIERpdmlzaW9uMSMwIQYDVQQDEExpUaGF3dGUgUGVyc29uYWwgUHJl
bWl1bSBDbTEqMCgGCSGSIb3DQEJARYbcGVyc29uYWwtdHJlbnW1bUB0aGF3dGUu
Y29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDJZtn4B0TPuYwu8KHvE0Vs
Bd/eJxZRNkERbGw77f4QfRKe5ZtCmv5gMcNmt3M6SK500Dl3Ili1DbbZ8/JE2dWI
Et12Tfla/G8jHnr2JhFTgcQ7xZCOEN1bUre4qrJMf8fAHB8Zs8QJQi6+u4A6UYD
ZicRFTuqW/KY3TZCstqlDQAQABoxMwETAPBgNVHRMBAf8EBTADAQH/MA0GCSqG
SIb3DQEBAUAA4GBAGk2ifc0KjNyL2071CKyuG+axTZmDhs8obF1Wub9NdP4qPIH
b4Vnjt4rueIXsDqg8A6iAJrf8xQVbrvlhVqYgPn/vnQdPfP+MCXRnzRn+qvxeTBh
KXLA4CxM+1bkOqhv5TJZUtt1KFBZDPgLGeSs2a+Wjs9Q2wfd6h+rM+D1KzGJ

-----END CERTIFICATE-----

Certificate Ingredients:

Data:

Version: 3 (0x2)

Serial Number: 0 (0x0)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting, OU=Certification Services Division, CN=Thawte Personal Premium CA/Email=personal-premium@thawte.com

Validity

Not Before: Jan 1 00:00:00 1996 GMT

Not After : Dec 31 23:59:59 2020 GMT

Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting, OU=Certification Services Division, CN=Thawte Personal Premium CA/Email=personal-premium@thawte.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:c9:66:d9:f8:07:44:cf:b9:8c:2e:f0:a1:ef:13:
45:6c:05:df:de:27:16:51:36:41:11:6c:6c:3b:ed:
fe:10:7d:12:9e:e5:9b:42:9a:fe:60:31:c3:66:b7:
73:3a:48:ae:4e:d0:32:37:94:88:b5:0d:b6:d9:f3:
f2:44:d9:d5:88:12:dd:76:4d:f2:1a:fc:6f:23:1e:
7a:f1:d8:98:45:4e:07:10:ef:16:42:d0:43:75:6d:
4a:de:e2:aa:c9:31:ff:1f:00:70:7c:66:cf:10:25:
08:ba:fa:ee:00:e9:46:03:66:27:11:15:3b:aa:5b:
f2:98:dd:36:42:b2:da:88:75

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

Signature Algorithm: md5WithRSAEncryption

69:36:89:f7:34:2a:33:72:2f:6d:3b:d4:22:b2:b8:6f:9a:c5:
36:66:0e:1b:3c:a1:b1:75:5a:e6:fd:35:d3:f8:a8:f2:07:6f:
85:67:8e:de:2b:b9:e2:17:b0:3a:a0:f0:0e:a2:00:9a:df:f3:
14:15:6e:bb:c8:85:5a:98:80:f9:ff:be:74:1d:3d:f3:fe:30:
25:d1:37:34:67:fa:a5:71:79:30:61:29:72:c0:e0:2c:4c:fb:
56:e4:3a:a8:6f:e5:32:59:52:db:75:28:50:59:0c:f8:0b:19:
e4:ac:d9:af:96:8d:2f:50:db:07:c3:ea:1f:ab:33:e0:f5:2b:
31:89

Thawte Premium Server CA-md5WithRSA

=====

MD5 Fingerprint: 06:9F:69:79:16:66:90:02:1B:8C:8C:A2:C3:07:6F:3A

PEM Data:

-----BEGIN CERTIFICATE-----

```

MIIDJzCCApCgAwIBAgIBATANBgkqhkiG9w0BAQQFADCBzjELMAkGA1UEBhMCWkEx
FTATBgNVBAGTDfDlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBUb3duMR0wGwYD
VQQKEXRUA GF3dGUgQ29uc3VsdGluZyBjYzEoMCMYGA1UECXMfQ2VydGlmaWNhdGlv
biBTZXJ2aWNlcyBEaXZpc2lvdjEhMB8GA1UEAxMYVGVhhd3RIIFByZW1pdW0gU2Vy
dmVylENBMSGwJgYJKoZIhvcNAQkBFHlwcmVtaXVtLXNlcnZlckB0aGF3dGUuY29t
MB4XDtk2MDgwMTAwMDAwMFoXDTIwMTIzMTIzNTk1OVowgc4xCzAJBgNVBAYTAipB
MRUwEwYDVQKIExwXZlXN0ZXJlENhcGUxEjAQBgNVBACTCUNhcGUgVG93bjEdMBsG
A1UEChMUUVGhhd3RIIENvbnN1bHRpbmcmY2MxKDAmbGVBAsTH0NlcnRpZmljYXRp
b24gU2VydmljZXMGRI2aXNpb24xITAFBgNVBAMTGFROYXd0ZSBQcmVtaXVtIFNI
cnZlciBDQTEoMCMYGCsqGSib3DQJEJARYZcHJlbWl1bS1zZXJ2ZXJAdGhhd3RlMnV
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA0jY2aovXwlue2oFBYo847kkE
VdbQ7xwblRZH7xhINTps9CtqBo87L+pW46+GjZ4X9560ZXUCTe/LCahUdib0GfQ
ug2SBhRz1JPLlyoAnFxDLz6FVL88kRu2hFKbgifLy3j+ao6hnO2RINYyIkFvYMR
uHM/qgeN9EJN50CdHDCaWEEAaMTMBEwDwYDVROTAQH/BAUwAwEB/zANBgkqhkiG
9w0BAQQFAAOBgQAmSCwWwlj66BZ0DKqqX1Q/8tfJeGBeXm43YyJ3Nn6yF8Q0ufUI
hfzJATj/Tb7yFkJD57taRvvBxhEf8UqwKEbJw8RCfbz6q1lu1bdRiBHjpIUZa4JM
pAwSremkrj/xw0llmozFyD4lt5SZu5IycQfwhl7tUCemDaYj+bvLpgcUQg==

```

-----END CERTIFICATE-----

Certificate Ingredients:

Data:

Version: 3 (0x2)

Serial Number: 1 (0x1)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Premium Server CA/Email=premium-server@thawte.com

Validity

Not Before: Aug 1 00:00:00 1996 GMT

Not After : Dec 31 23:59:59 2020 GMT

Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Premium Server CA/Email=premium-server@thawte.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:d2:36:36:6a:8b:d7:c2:5b:9e:da:81:41:62:8f:
38:ee:49:04:55:d6:d0:ef:1c:1b:95:16:47:ef:18:
48:35:3a:52:f4:2b:6a:06:8f:3b:2f:ea:56:e3:af:
86:8d:9e:17:f7:9e:b4:65:75:02:4d:ef:cb:09:a2:
21:51:d8:9b:d0:67:d0:ba:0d:92:06:14:73:d4:93:
cb:97:2a:00:9c:5c:4e:0c:bc:fa:15:52:fc:f2:44:
6e:da:11:4a:6e:08:9f:2f:2d:e3:f9:aa:3a:86:73:
b6:46:53:58:c8:89:05:bd:83:11:b8:73:3f:aa:07:
8d:f4:42:4d:e7:40:9d:1c:37

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

Signature Algorithm: md5WithRSAEncryption

26:48:2c:16:c2:58:fa:e8:16:74:0c:aa:aa:5f:54:3f:f2:d7:
c9:78:60:5e:5e:6e:37:63:22:77:36:7e:b2:17:c4:34:b9:f5:
08:85:fc:c9:01:38:ff:4d:be:f2:16:42:43:e7:bb:5a:46:fb:
c1:c6:11:1f:f1:4a:b0:28:46:c9:c3:c4:42:7d:bc:fa:ab:59:
6e:d5:b7:51:88:11:e3:a4:85:19:6b:82:4c:a4:0c:12:ad:e9:
a4:ae:3f:f1:c3:49:65:9a:8c:c5:c8:3e:25:b7:94:99:bb:92:

32:71:07:f0:86:5e:ed:50:27:a6:0d:a6:23:f9:bb:cb:a6:07:

14:42

Thawte Server CA-md5WithRSA

=====

MD5 Fingerprint: C5:70:C4:A2:ED:53:78:0C:C8:10:53:81:64:CB:D0:1D

PEM Data:

-----BEGIN CERTIFICATE-----

```

MIIDEzCCAnygAwIBAgIBATANBgkqhkiG9w0BAQQFADCBxDELMAkGA1UEBhMCWkEx
FTATBgNVBAGTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBUb3duMR0wGwYD
VQKExRUaGF3dGUgQ29uc3VsdGluZyBjYzEoMCMYGA1UECXMfQ2VydGlmaWNhdGlv
biBTZXJ2aWNlcyBEaXZpc2lvbjEZMBCGA1UEAxMQVGVhd3RlIFNlcnZlciBDQTEu
MCQGCSqGSIsb3DQEJARYXc2VydmVyLWNLcnRzQHRoYXN0ZS5jb20wHhcNOTYwODAx
MDAwMDAwWhcNMjAxMjMjMjM1OTU5WjCBxDELMAkGA1UEBhMCWkExFTATBgNVBAGT
DFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBUb3duMR0wGwYDVQKExRUaGF3
dGUgQ29uc3VsdGluZyBjYzEoMCMYGA1UECXMfQ2VydGlmaWNhdGlvbiBTZXJ2aWNl
cyBEaXZpc2lvbjEZMBCGA1UEAxMQVGVhd3RlIFNlcnZlciBDQTEuMCQGCSqGSIsb3
DQEJARYXc2VydmVyLWNLcnRzQHRoYXN0ZS5jb20wZGZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBANOkUG7I/1Zr5s9dtuoMaHVHoqrC2oQl/Kj0R1HahbUgdJSGHg91
yekIYfUGbTBuFRkC6VLAYttNmZ7iagxEOM3+vuNkCXDF/rFrKbYvScg71CcEJRCX
L+eQbcAoQpnXTEPew/UhbVSfXcNY4cDk2VuwuNy0e9820sK1ZiS1ocNAGMBAAGj
EzARMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQEEBQADgYEAB/pMaVz7lcxG
7oWDTSEwjsrZqG9JGubaUeNgcGyEYRGhGshIPIldfU+VPaGLtwtimHp1it2ITk6e
QNuoZDJ0uW8NxuOzRAvZim+aKZuZGCg70eNAKJpaPNW15yAbi8qkq43pUdniTCxZ
qdq5snUb9kLy78fyGPMjvKP/iiMucEc=

```

-----END CERTIFICATE-----

Certificate Ingredients:

Data:

Version: 3 (0x2)

Serial Number: 1 (0x1)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Server CA/Email=server-certs@thawte.com

Validity

Not Before: Aug 1 00:00:00 1996 GMT

Not After : Dec 31 23:59:59 2020 GMT

Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Server CA/Email=server-certs@thawte.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
3a:c2:b5:66:22:12:d6:87:0d

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

Signature Algorithm: md5WithRSAEncryption

07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:

4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
70:47

Supported Thawte SHA1 Based Root Certificates

- [Thawte Personal Basic CA-sha1WithRSA](#)
- [Thawte Personal Freemail CA-sha1WithRSA](#)
- [Thawte Personal Premium CA-sha1WithRSA](#)
- [Thawte Premium Server CA-sha1WithRSA](#)
- [Thawte Server CA-sha1WithRSA](#)

Thawte Personal Basic CA-sha1WithRSA

=====

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

0d:8e:15:12:e1:ac:bb:77:8d:38:e3:24:df:8c:30:f2

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting, OU=Certification Services Division, CN=Thawte Personal Basic CA/emailAddress=personal-basic@thawte.com

Validity

Not Before: Jan 1 00:00:00 1996 GMT

Not After : Jan 1 23:59:59 2021 GMT

Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting, OU=Certification Services Division, CN=Thawte Personal Basic CA/emailAddress=personal-basic@thawte.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:bc:bc:93:53:6d:c0:50:4f:82:15:e6:48:94:35:

a6:5a:be:6f:42:fa:0f:47:ee:77:75:72:dd:8d:49:

9b:96:57:a0:78:d4:ca:3f:51:b3:69:0b:91:76:17:

22:07:97:6a:c4:51:93:4b:e0:8d:ef:37:95:a1:0c:

4d:da:34:90:1d:17:89:97:e0:35:38:57:4a:c0:f4:
08:70:e9:3c:44:7b:50:7e:61:9a:90:e3:23:d3:88:
11:46:27:f5:0b:07:0e:bb:dd:d1:7f:20:0a:88:b9:
56:0b:2e:1c:80:da:f1:e3:9e:29:ef:14:bd:0a:44:
fb:1b:5b:18:d1:bf:23:93:21

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

Signature Algorithm: sha1WithRSAEncryption

88:3b:fe:b8:f9:7a:42:46:11:a0:a4:a2:64:85:cd:48:1c:9c:
d5:8a:51:cd:2f:c1:7d:b1:07:cf:d7:01:de:32:3f:96:e4:84:
fe:d1:5e:ad:0c:7e:0e:63:49:6a:0e:10:e4:97:d0:3f:c5:a7:
29:d9:a6:53:1e:4b:1e:3f:54:fa:c0:84:35:73:ea:91:a9:dc:
5d:93:57:05:06:0c:07:b9:af:0b:44:39:88:21:a0:ee:82:73:
a9:46:2f:69:6c:25:74:a9:cd:df:a7:d7:fd:85:30:04:94:35:
4a:a7:1b:33:24:2c:44:16:ed:0a:c4:df:80:aa:65:1a:bf:71:
26:f0

-----BEGIN CERTIFICATE-----

MIIDMDCCApmgAwIBAgIQDY4VEuGsu3eNOOMk34ww8jANBgkqhkiG9w0BAQUFADCB
yzELMAkGA1UEBhMCWkExFTATBgNVBAGwTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJ
Q2FwZSBub3duMR0wGAYDVQQKEwFuGF3dGUgQ29uc3VsdGluZzEoMCMYGA1UECzMf
Q2VydGlmaWNhdGlvbiBTZXJ2aWNlcyBEaXZpc2lvbEhMB8GA1UEAxMYVGVhd3RI
IFBlcnNvbmlEJhc2lJlENBMSgwJgYJKoZIhvcNAQkBFhWZlZj25hbC1iYXNp
Y0B0aGF3dGUuY29tMB4XDTE2MDEwMTAwMDAwMFoXDTE2MDEwMTIzNTk1OVowgc3x
CzAJBgNVBAYTAlpBMRUwEwYDVQQIEwVYDVQKIExwXZXN0ZXJlENhcGUxEjAQBgNVBAcTCUNh
cGUgVG93bjEaMBGA1UEChMRVGVhd3RIlENvbnN1bHRpbmcxKDAmbGVBASTh0NI
cnRpb24gU2VydmljZXMgRGI2aXNpb24xITAfBgNVBAMTGFRoYXc0ZSBQ
ZXJzb25hbC1iYXNpYyBDQTEoMCMYGCsqGSib3DQEJARYZcGVyc29uYWwtYmFzaWNA

```

dGhhd3RlLmNvbTCBnzANBkgqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuLyTU23AUE+C
FeZIIDWmWr5vQvoPR+53dXLdjUmblllegeNTP1GzaQuRdhciB5dqxFGTS+CN7zeV
oQxN2jSQHReJl+A1OFdKwPQIcOk8RHtQfmGakOMj04gRRif1CwcOu93RfyAKiLIW
Cy4cgNrx454p7xS9CkT7G1sY0b8jkyECAwEAAaMTMBEwDwYDVR0TAQH/BAUwAwEB
/zANBkgqhkiG9w0BAQUFAAOBgQCIO/64+XpCRhGgpKJkhc1IHJzVilHNL8F9sQfP
1wHeMj+W5IT+0V6tDH4OY0lqDhDkl9A/xacp2aZTHkseP1T6wIQ1c+qRqdxdk1cF
BgwHua8LRDmllaDugnOpRi9pbCV0qc3fp9f9hTAEIDVKpxszJCxEFu0KxN+AqmUa
v3Em8A==
-----END CERTIFICATE-----

```

Thawte Personal Freemail CA-sha1WithRSA

=====

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

12:3d:f0:e7:da:2a:22:47:a4:38:89:e0:8a:ee:c9:67

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting, OU=Certification Services Division, CN=Thawte Personal Freemail CA/emailAddress=personal-freemail@thawte.com

Validity

Not Before: Jan 1 00:00:00 1996 GMT

Not After : Jan 1 23:59:59 2021 GMT

Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting, OU=Certification Services Division, CN=Thawte Personal Freemail CA/emailAddress=personal-freemail@thawte.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:d4:69:d7:d4:b0:94:64:5b:71:e9:47:d8:0c:51:
 b6:ea:72:91:b0:84:5e:7d:2d:0d:8f:7b:12:df:85:
 25:75:28:74:3a:42:2c:63:27:9f:95:7b:4b:ef:7e:
 19:87:1d:86:ea:a3:dd:b9:ce:96:64:1a:c2:14:6e:
 44:ac:7c:e6:8f:e8:4d:0f:71:1f:40:38:a6:00:a3:
 87:78:f6:f9:94:86:5e:ad:ea:c0:5e:76:eb:d9:14:
 a3:5d:6e:7a:7c:0c:a5:4b:55:7f:06:19:29:7f:9e:
 9a:26:d5:6a:bb:38:24:08:6a:98:c7:b1:da:a3:98:
 91:fd:79:db:e5:5a:c4:1c:b9

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

Signature Algorithm: sha1WithRSAEncryption

1e:98:60:d4:e5:f2:54:60:b0:3d:1a:81:64:47:f7:5b:a3:d9:
 6f:c3:29:0b:a7:d2:a9:81:49:f6:c3:6d:85:14:28:45:44:01:
 f4:71:5c:95:2e:14:0f:1a:2b:d1:a9:6b:c1:5f:67:3d:16:f1:
 72:20:af:be:16:ca:0e:30:5f:c9:cb:a5:93:2c:c3:67:54:1e:
 72:22:8a:23:76:6c:94:1d:51:52:6c:9d:c4:e0:47:02:d7:cc:
 bf:f0:80:7b:18:6e:25:dc:62:61:d6:a6:fe:c1:1d:7f:d9:b3:
 fd:8d:5c:45:10:5a:c6:65:64:9a:eb:2c:f5:03:4f:d6:48:62:
 fb:2e

-----BEGIN CERTIFICATE-----

MIIDPDCCAqWgAwIBAgIQEj3w59oqlkekOIngiu7JZzANBgkqhkiG9w0BAQUFADCB
 0TElMAkGA1UEBhMCWkExFTATBgNVBAGTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJ
 Q2FwZSBUB3duMR0wGAYDVQQKExFUaGF3dGUgQ29uc3VsdGluZzEoMCMYGA1UECXMf
 Q2VydGlmaWNhdGlvbiBTZXJ2aWNlcyBEaXZpc2lvb2JkMCIGA1UEAxMbvGhhd3RI
 IFBlcnNvb2F0aGF3dGUuY29tMB4XDTEwMTAwMDAwMFOxDTIxMDEwMTIzNTk1
 cmVlbWFpbEB0aGF3dGUuY29tMB4XDTEwMTAwMDAwMFOxDTIxMDEwMTIzNTk1

OVowgdExCzAJBgNVBAYTAIpBMRUwEwYDVQQIEwxXZXR0ZXJlENhcGUxEjAQBgNV
 BAACUNhcGUgV93bjEaMBGGA1UEChMRVGVhd3RlIENvbnN1bHRpbmcxKDAmBgNV
 BAsTH0NlcnRpZmljYXRpb24gU2VydmljZXMgRGI2aXNpb24xJDAiBgNVBAMTG1Ro
 YXd0ZSBQZXJzb25hbCBGcmVlbWFpbCBDQTErMCKGCSqGSIb3DQEJARYccGVyc29u
 YWwtZnJlZW1haWxAdGhhd3RlLmNvbTcBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
 gYEA1GnX1LCUZFTx6UfYDFG26nKRslRefs0Nj3sS34UldSh0OkIsYyeflXtL734Z
 hx2G6qPduc6WZBrCFG5ErHzmj+hND3EfQDimAKOHePb5IIZererAXnbr2RSjXW56
 fAylS1V/Bhkpf56ajtVquzkgCGqYx7Hao5iR/Xnb5VrEHLkCAwEAAaMTMBEwDwYD
 VR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQUFAAOBgQAemGDU5fJUyLA9GoFkr/db
 o9lwvykLp9KpgUn2w22FFChFRAH0cVyVlHQPgIvRqWvBX2c9FvFyIK++FsoOMF/J
 y6WTLMNnVB5yloojdmyUHVFSbJ3E4EcC18y/8IB7GG4l3GJh1qb+wR1/2bP9jVxF
 EFrGZWSa6yz1A0/WSGL7Lg==
 -----END CERTIFICATE-----

Thawte Personal Premium CA-sha1WithRSA

=====

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

40:05:b2:53:a0:1a:46:43:50:09:81:8f:12:10:76:ec

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting, OU=Certification Services
 Division, CN=Thawte Personal Premium CA/emailAddress=personal-premium@thawte.com

Validity

Not Before: Jan 1 00:00:00 1996 GMT

Not After : Jan 1 23:59:59 2021 GMT

Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting, OU=Certification Services
 Division, CN=Thawte Personal Premium CA/emailAddress=personal-premium@thawte.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:c9:66:d9:f8:07:44:cf:b9:8c:2e:f0:a1:ef:13:
45:6c:05:df:de:27:16:51:36:41:11:6c:6c:3b:ed:
fe:10:7d:12:9e:e5:9b:42:9a:fe:60:31:c3:66:b7:
73:3a:48:ae:4e:d0:32:37:94:88:b5:0d:b6:d9:f3:
f2:44:d9:d5:88:12:dd:76:4d:f2:1a:fc:6f:23:1e:
7a:f1:d8:98:45:4e:07:10:ef:16:42:d0:43:75:6d:
4a:de:e2:aa:c9:31:ff:1f:00:70:7c:66:cf:10:25:
08:ba:fa:ee:00:e9:46:03:66:27:11:15:3b:aa:5b:
f2:98:dd:36:42:b2:da:88:75

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

Signature Algorithm: sha1WithRSAEncryption

ba:64:0a:e8:f3:b4:31:c9:27:6f:a2:76:a0:2d:36:71:c7:86:
c0:08:c2:4e:ed:da:9a:24:19:87:fc:5a:23:9c:72:4d:08:df:
ad:5c:c3:3b:24:81:1d:57:8f:b6:12:a5:22:03:ef:12:bd:d1:
2d:5e:96:8f:26:26:4f:4b:1b:7c:3b:a0:52:1a:a5:a8:37:86:
c4:47:2a:ca:dd:41:f8:68:f5:c2:13:41:29:9a:f0:0c:a8:cd:
a1:fc:15:23:02:db:7a:2b:d4:62:51:42:47:c4:a3:1f:f4:d2:
c5:4d:54:10:eb:da:f0:cc:a7:4f:37:0c:bd:3c:cb:10:e3:1a:
e8:15

-----BEGIN CERTIFICATE-----

MIIDODCCAqGgAwIBAgIQQAWyU6AaRkNQCYGPEhB27DANBgkqhkiG9w0BAQUFADCB
zzELMAkGA1UEBhMCWkExFTATBgNVBAGTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJ

Q2FwZSBUb3duMRowGAYDVQKExFUaGF3dGUgQ29uc3VsdGluZzEoMCMYGA1UECXMf
 Q2VydGhmaWNhdGlvbiBTXJ2aWNlcyBEaXZpc2lvbEjMCEGA1UEAxMaVGhhd3RI
 IFBicnNvbWVzIFByZW1pdW0gQ0ExKjAoBkgkqhkG9w0BCQEWG3BlcnNvbWVzLXBy
 ZW1pdW1AdGhhd3RlMnNvbTAeFw05NjAxMDEwMDAwMDBaFw0yMTAxMDEyMzU5NTla
 MIHPMQswCQYDVQGEwJaQTEVMBMGA1UECBMMV2VzdGVybiBDYXBIMRIwEAYDVQQH
 EwIDYXBIIFRvd24xGjAYBgNVBAoTEVRoYXZ0ZSBDb25zdWx0aW5nMSgwJgYDVQQQL
 Ex9DZXJ0aWZpY2F0aW9uIFNlcnZpY2VzIERpdmlzaW9uMSMwIQYDVQQDEExpUaGF3
 dGUgUGVyc29uYWwgUHJlbWl1bSBDQTEqMCGGCSqGSIb3DQEJARYbcGVyc29uYWwt
 cHJlbWl1bUB0aGF3dGUuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDJ
 Ztn4B0TPuYwu8KHvE0VsBd/eJxZRNkERbGw77f4QfRKe5ZtCmv5gMcNmt3M6SK5O
 0DI3Ili1Dbbz8/JE2dWIEt12Tfla/G8jHnrX2JhFTgcQ7xZC0EN1bUre4qrJMf8f
 AHB8Zs8QJQI6+u4A6UYDZicRFTuqW/KY3TZCstqldQIDAQABoxMwETAPBgNVHRMB
 Af8EBTADAQH/MA0GCSqGSIb3DQEBAQUAA4GBALpkCujztDHJJ2+idqAtNnHHhsAI
 wk7t2pokGYf8WiOcck0I361cwzskgR1Xj7YSpSID7xK90S1elo8mJk9LG3w7oFla
 pag3hsRHksrdQfho9cITQsma8AyozaH8FSMC23or1GJRQkfEox/00sVNVBDr2vDM
 p083DL08yxDjGugV
 -----END CERTIFICATE-----

Thawte Premium Server CA-sha1WithRSA

=====

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

36:12:22:96:c5:e3:38:a5:20:a1:d2:5f:4c:d7:09:54

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Premium Server CA/emailAddress=premium-server@thawte.com

Validity

Not Before: Aug 1 00:00:00 1996 GMT

Not After : Jan 1 23:59:59 2021 GMT

Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Premium Server CA/emailAddress=premium-server@thawte.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:d2:36:36:6a:8b:d7:c2:5b:9e:da:81:41:62:8f:
38:ee:49:04:55:d6:d0:ef:1c:1b:95:16:47:ef:18:
48:35:3a:52:f4:2b:6a:06:8f:3b:2f:ea:56:e3:af:
86:8d:9e:17:f7:9e:b4:65:75:02:4d:ef:cb:09:a2:
21:51:d8:9b:d0:67:d0:ba:0d:92:06:14:73:d4:93:
cb:97:2a:00:9c:5c:4e:0c:bc:fa:15:52:fc:f2:44:
6e:da:11:4a:6e:08:9f:2f:2d:e3:f9:aa:3a:86:73:
b6:46:53:58:c8:89:05:bd:83:11:b8:73:3f:aa:07:
8d:f4:42:4d:e7:40:9d:1c:37

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

Signature Algorithm: sha1WithRSAEncryption

65:90:ac:88:0f:56:d9:e6:30:34:d4:26:c7:d0:50:f1:92:de:
6b:d4:39:88:09:22:c6:a6:63:83:03:f7:99:77:d8:b2:e5:18:
b8:5d:63:f3:d4:73:fb:6c:9c:99:78:f1:4b:78:7d:19:24:c3:
2b:02:84:f8:bc:22:d9:8a:22:d7:a0:fc:71:ec:91:87:20:f1:
b8:ec:b1:e5:55:80:ac:3d:52:c8:39:0e:c2:f0:c0:05:4f:d6:
82:75:8c:bd:5f:d2:dc:76:9a:05:12:c9:af:72:c3:dc:25:7e:
a4:4d:8e:17:a5:e0:87:7f:e1:9a:5a:e1:60:dc:64:23:3c:42:
2e:4d

-----BEGIN CERTIFICATE-----

```

MIIDNjCCAp+gAwIBAgIQNhilsXjOKUgodJfTncJVDANBgkqhkiG9w0BAQUFADCB
zjELMAkGA1UEBhMCWkExFTATBgNVBAGTDfDlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJ
Q2FwZSBUb3duMR0wGwYDVQQKEXRUAzF3dGUgQ29uc3VsdGluZyBjYzEoMCMYGA1UE
CxMfQ2VydGlmYWVhdGlvbiBTZXJ2aWNlcyBEaXZpc2lvbjEhMB8GA1UEAxMYVGVhd
d3RIIFByZW1pdW0uU2VydmlvYlENBMSGwJgYJKoZIhvcNAQkBFhlwcmVtaXVtLXNI
cnZlckB0aGF3dGUuY29tMB4XDTk2MDgwMTAwMDAwMFoXDTEwMDEwMTIzNTk1OVow
gc4xCzAJBgNVBAYTAjpBMRUwEwYDVQQIEwxxZXN0ZXJ1eENhcGUxEjAQBgNVBAcT
CUNhcGUgVG93bjEdMBsGA1UEChMUUVGVhdh3RIENvbnN1bHRpbmVtY2MxKDAmbG93
BAsTH0NlcnRpZmljYXRpb24gU2VydmljZXMGZGl2aXNpb24xITAfBgNVBAMTGFRO
YXd0ZSBUcmVtaXVtIFNlcnZlciBDQTEoMCMYGCsGSIb3DQEJARYZcHJlbWI1bS1z
ZXJ2ZXJAdGhhd3RlLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA0jY2
aovXwlue2oFBYo847kkEVdbQ7xwblRZH7xhINTpS9CtqBo87L+pW46+GjZ4X9560
ZXUCTe/LCAlhUdib0GfQug2SBhRz1JPLIyoAnFxODLz6FVL88kRu2hFKbgifLy3j
+ao6hnO2RINyYkFvYMRuHM/qgeN9EJN50CdHDCaWEEAaMTMBEwDwYDVR0TAQH/
BAUwAwEB/zANBgkqhkiG9w0BAQUFAAOBjQBlkKyID1bZ5jA01CbH0FDxkt5r1Dml
CSLGpmODA/eZd9iy5Ri4XWPz1HP7bJyZePFLeH0ZJMMrAoT4vCLZiiLXoPxx7JGH
IPG47LHIVYCsPVLIOQ7C8MAFT9aCdYy9X9LcdpoFEsmvcsPcJX6kTY4XpeCHf+Ga
WuFg3GQjPEluTQ==

```

-----END CERTIFICATE-----

Thawte Server CA-sha1WithRSA

=====

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

34:a4:ff:f6:30:af:4c:a5:3c:33:17:42:a1:94:66:75

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Server CA/emailAddress=server-certs@thawte.com

Validity

Not Before: Aug 1 00:00:00 1996 GMT

Not After : Jan 1 23:59:59 2021 GMT

Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Server CA/emailAddress=server-certs@thawte.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
3a:c2:b5:66:22:12:d6:87:0d

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

Signature Algorithm: sha1WithRSAEncryption

be:40:69:41:6f:c6:db:c1:a7:bf:07:c0:45:e4:d0:b5:43:1e:
4c:95:33:35:e9:5e:c2:3e:28:f6:a8:0d:50:d5:ff:e2:0c:0f:
fc:50:02:8e:ae:91:b9:ad:34:8a:8d:9f:27:71:aa:19:cc:4b:
e8:04:ca:d4:17:6b:12:1a:d6:c6:5f:d6:cd:5e:ff:89:76:bf:
d8:48:d8:59:bd:08:8a:89:1d:57:cd:45:1e:52:ba:12:9a:84:

fa:18:89:5f:e8:f9:30:35:6a:01:60:b9:99:80:83:85:0a:6e:

da:f4:c9:8f:5e:73:2d:31:4a:63:a0:74:f2:1f:8b:22:d2:29:

3e:eb

-----BEGIN CERTIFICATE-----

MIIDijCCAougAwIBAgIQNKT/9jCvTKU8MxdCoZRmdTANBgkqhkiG9w0BAQUFADCB
xDELMAkGA1UEBhMCWkExFTATBgNVBAGTDfDlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJ
Q2FwZSBUb3duMR0wGwYDVQQKExRUaGF3dGUgQ29uc3VsdGluZyBjYzEoMCMYGA1UE
CxMfQ2VydGlmawNhdGlvbiBTZXJ2aWNlcyBEaXZpc2lvbjEZMBCGA1UEAxMQVGhh
d3RIIFNlcnZlciBDQTEEmMCQGCSqGSIb3DQEJARYXc2VydmVyLWNIcnRzQHRoYXd0
ZS5jb20wHhcNOTYwODAwMDAwMDAwWhcNMjEwMTAxMjM1OTU5WjCBxDELMAkGA1UE
BhMCWkExFTATBgNVBAGTDfDlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBUb3du
MR0wGwYDVQQKExRUaGF3dGUgQ29uc3VsdGluZyBjYzEoMCMYGA1UECXMfQ2VydGlm
awNhdGlvbiBTZXJ2aWNlcyBEaXZpc2lvbjEZMBCGA1UEAxMQVGhhhd3RIIFNlcnZl
ciBDQTEEmMCQGCSqGSIb3DQEJARYXc2VydmVyLWNIcnRzQHRoYXd0ZS5jb20wgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANOkUG7l/1Zr5s9dtuoMaHVHoqrC2oQl
/Kj0R1HahbUgdJSGHg91yeklYfUGbTBuFRkC6VLAYttNmZ7iagxEOM3+vuNkCXDF
/rFrKbYvScg71CcEJRCXL+eQbcAoQpnXTEPew/UhbVSfXcNY4cDk2VuwuNy0e982
OsK1ZiS1ocNAGMBAAGjEzARMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQEF
BQADgYEAvkBpQW/G28GnvwfAReTQtUMeTJUzNelewj4o9qgNUNX/4gwP/FACjq6R
ua00io2fj3GqGcxL6ATK1BdrEhrWxl/WzV7/iXa/2EjYWb0liokdV81FHIK6EppE
+hiJX+j5MDVqAWC5mYCDhQpu2vTJj15zLTFKY6B08h+LltlpPus=

-----END CERTIFICATE--