SPA Certificate Authority (CA) List

Document

Tue, 01/27/2015 - 05:43

Patrick Born 8 years ago

Cisco SPA series phones and ATAs can use certificate-authenticated HTTPS (SSL) sessions to ensure secure provisioning. For a provisioning server to be acceptable to the SPA phone or ATA, the server must present a certificate signed by Cisco's Certificate Authority (CA).

Over the years, we have added certificate authorities (CA) as needed and for administrative reasons.

If your SPA1xx or SPA232D ATA or SPA5xx IP Phone is running current or newer firmware, 1.3.3 or 7.5.6 respectively, use the newer "Cisco 2k Small Business CA" even though you could use any of the older CAs.

A HTTPS server used for device provisioning must use a certificate signed by the appropriate CA for the device.

To obtain this certificate, you must submit a certificate signing request (CSR) by following the CSR instructions.

When submitting the CSR, you must list the device types that you want to provision so we know what certificates to generate for you.

Following is a list to help you identify the appropriate CA associated with your device:

- **Cisco 2k Small Business CA:**
  - SPA1xx firmware 1.3.3 and newer
    (SPA112 and SPA122)
  - SPA232D firmware 1.3.3 and newer
  - SPA5xx firmware 7.5.6 and newer
    (SPA501G, SPA502G, SPA504G, SPA508G, SPA509G, SPA512G, SPA514G, SPA525G, and SPA525G2)
- **Cisco Small Business (SB) CA:**
  - SPA1xx (SPA112 and SPA122)
  - SPA232D
  - SPA3xx (SPA301 and SPA303)
  - SPA5xx (SPA501G, SPA502G, SPA504G, SPA508G, SPA509G, SPA512G, SPA514G, SPA525G, and SPA525G2)
  - SRP5xx (SRP521 and SRP541)
- **Linksys CA:**
  - PAP2
  - WRTP
  - RTP
- **Sipura CA:**
  - PAP2T
  - WRP400
  - SPA2xxx (SPA2000 and SPA2102)
  - SPA3xxx (SPA3000 and SPA3102

Note:

A HTTPS server can only present a single certificate per **IP address:port**

To securely provision devices associated with multiple CAs, you will need to implement multiple HTTPS services. You can use any one or a combination of the following options:

- Deploy multiple computers with one network interface card (NIC) per computer, each performing the role of a CA

Example:

- https://computerA:443/spa$MA.cfg
- https://computerB:443/spa$MA.cfg

- Deploy a single computer with multiple NICs where each NIC has a unique IP address where each IP address performs the role of a unique CA

Example:

- https://computerAnic1:443/spa$MA.cfg
- https://computerAnic2:443/spa$MA.cfg

- Deploy a single computer with a single NIC where unique ports are used and each unique port is associated with a unique CA

- https://computerA:443/spa$MA.cfg
- https://computerA:3443/spa$MA.cfg

<end of original document>

<Start of note from >

Informations in such documents seems to be either obsolete or invalid from scratch. Most devices accept more than one CA, so multiple HTTPS server as suggested by document may be overkill in some cases. But I will leave original ocument above, because I can't test all types and firmware versions.

See table bellow for real cross-compatibility list. It is based on real test of mentioned devices.

Device \ CA	Linksys CA	Sipura CA	Cisco SB CA	Verisign
PAP2T, 5.1.6(LS)	OK	OK	~~NO~~	~~NO~~
SPA112, 1.3.1(003)	OK	OK	OK	~~NO~~
SPA232D, 1.3.1(003_240)	OK	OK	OK	~~NO~~
SPA-962, 6.1.5(a)	OK	OK	~~NO~~	?
SPA508G, 7.5.4	OK	OK	OK	~~NO~~
SPA525G2, 7.5.4	OK	OK	OK	?

```
Note:

Linksys CA:

/C=US/ST=California/L=Irvine/O=Cisco Linksys, LLC./OU=Cisco Linksys Certificate Authority

/CN=Cisco Linksys Provisioning Root Authority 1/emailAddress=linksys-certadmin@cisco.com
```

/C=US/ST=California/L=San Jose/O=Sipura Technology, Inc./OU=Sipura Technology Certificate Authority

/CN=Sipura Technology Provisioning Root Authority 1/emailAddress=webmaster@sipura.com

Serial: 45:BF:48:C0:CE:B8:8F:7B:C8:E1:6D:85:62:5A:5B:8F

CiscoSB CA:

/C=US/ST=California/L=San Jose/O=Cisco Small Business/OU=Cisco Small Business Certificate Authority

/CN=Cisco Small Business Provisioning Root Authority 1/emailAddress=ciscosb-certadmin@cisco.com

Serial: D0:7D:8C:15:C0:BA:7C:B6:44:69:98:B1:EA:89:87:9F

Verisign CA (based on informations in SPA5xx IP Phone 7.x Firmware Update Information):

/C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority

Serial: 70:BA:E4:1D:10:D9:29:34:B6:38:CA:7B:03:CC:BA:BF

or

/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=Terms of use at https://www.verisign.com/rpa (c)05

/CN=VeriSign Class 3 Secure Server CA

Serial: 75:33:7D:9A:B0:E1:23:3B:AE:2D:7D:E4:46:91:62:D4

Note: according Verisign (now Symantec) tech support, VeriSign Class 3 Secure Server CA based certificates are no longer issued. Class 3 Public Primary Certification Authority rooted certificates are sold under product name "Secure Site" and "Secure Site Pro".

★★★★☆ Overall Rating: 4 (1 ratings)

Log in or register to post comments

Comments

Collapse all Recent replies first

Dan Lukes 7 years ago

★

I see no SPA232D in document at all, althougth it seems the document apply to it as well.

Log in or register to post comments

Dan Lukes 6 years ago

★

Today I got brand new SPA508G phone. It has been shipped with 7.5.2 firmware and it's client certificate is issued by

```
/C=US/ST=California/L=San Jose/O=Cisco Small Business/OU=Cisco Small Business Certificate Authority/CN=Cisco Small Business Client Root Authority 2/emailAddress=ciscosb-certadmin@cisco.com
Serial: d0:7d:8c:15:c0:ba:7c:b6:44:69:98:b1:ea:89:87:9f
```

authority. Our secure provisioning doesn't work with the device (the phone can connect to provisioning server, but we are unable to identify the phone as we are unable to verify the client certificate).

As far as I know, there is no announcement from Cisco related to it. Nor even there is the root certificate of such authority published.

Oh dear Cisco ...

See More Log in or register to post comments

cisco@provu.co.uk 5 years ago

Did you get to the bottom of this?

I'm also struggling with SPA502 with 7.5.2. firmware.

See More Log in or register to post comments

Dan Lukes 5 years ago
★

Its easy to solve the issue. You need to obtain the new CA certificate and add it to bundle of certificates your's provisioning system is already supporting. I did it the same day I has been affected by issue.

The problem is not the issue itself. The problem is the change is not properly documented nor announced by Cisco and the required CA certificate is not available to public.

See More Log in or register to post comments

cisco@provu.co.uk 5 years ago

Yes, came to the same conclusion just now. My combinedca.crt is missing the new CA. My server certificates are fine.

I've emailed cisco so hopefully I'll get the new CA back soon.

Agree some notice on changes is good.

Log in or register to post comments

cisco@provu.co.uk 5 years ago

If you could email me your CA file, that would save me waiting for cisco. Only if you have it handy and its easy. Thanks

See More Log in or register to post comments

Dan Lukes 5 years ago
★

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            d0:7d:8c:15:c0:ba:7c:b6:44:69:98:b1:ea:89:87:9f
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=California, L=San Jose, O=Cisco Small Business, OU=Cisco Small Business Certificate Authority, CN=Cisco Small Business Client Root
Authority 2/emailAddress=ciscosb-certadmin@cisco.com
```

```
            Not Before: Aug  2 22:37:43 2013 GMT
            Not After : Jun 28 22:37:43 2035 GMT
        Subject: C=US, ST=California, L=San Jose, O=Cisco Small Business, OU=Cisco Small Business Certificate A           co Small
Authority 2/emailAddress=ciscosb-certadmin@cisco.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:bf:c2:f8:3a:e6:c6:89:21:8c:82:a0:79:91:73:
                    72:f3:74:d5:a8:4e:a7:3d:7b:02:ab:6b:2c:8d:71:
                    82:02:76:7a:fa:bf:2e:8c:e7:b0:47:15:96:ab:83:
                    8f:48:0d:e7:e7:15:f2:ed:54:2e:cd:7d:e3:36:34:
                    f6:eb:05:a3:d5:39:57:2e:6a:ee:b2:0a:b7:7b:a6:
                    dd:82:e9:6a:94:01:2f:89:1d:52:93:f4:ec:23:08:
                    ae:6f:04:0a:94:5d:92:94:d6:3a:c4:58:69:da:2b:
                    2e:64:cf:77:0e:29:82:c3:be:7d:7a:eb:f8:f4:d1:
                    5c:18:77:85:a4:5e:e8:1e:51:f6:d4:79:f1:e1:c8:
                    44:7c:67:ad:9c:f7:9b:80:74:1f:32:05:79:c3:d5:
                    67:41:df:1c:80:9a:10:57:80:9b:7e:ab:e6:50:24:
                    82:42:06:cf:df:34:7d:0a:e9:70:56:dc:6f:0a:c5:
                    1b:32:7a:f0:e1:73:2e:21:d4:92:7a:d6:53:96:83:
                    b3:8d:82:bc:7f:5e:03:ed:e9:7e:63:39:bb:37:0a:
                    c6:32:c7:fe:db:3f:b0:8a:02:85:83:78:2a:87:32:
                    5a:b1:82:ff:38:df:0d:4b:83:31:8e:af:78:e6:79:
                    46:94:8e:2e:c3:18:34:36:31:90:b6:3a:89:1e:06:
                    1a:67
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                F8:C2:33:67:A9:12:FC:5D:43:23:9E:55:D3:7E:57:40:1A:55:42:10
            X509v3 Authority Key Identifier:
                keyid:F8:C2:33:67:A9:12:FC:5D:43:23:9E:55:D3:7E:57:40:1A:55:42:10
                DirName:/C=US/ST=California/L=San Jose/O=Cisco Small Business/OU=Cisco Small Business Certificate Authority/CN=Cisco Small Business Client
Root Authority 2/emailAddress=ciscosb-certadmin@cisco.com
                serial:D0:7D:8C:15:C0:BA:7C:B6:44:69:98:B1:EA:89:87:9F

            X509v3 Basic Constraints:
                CA:TRUE
            Netscape Cert Type:
                SSL CA
            X509v3 Extended Key Usage:
                TLS Web Client Authentication
    Signature Algorithm: sha1WithRSAEncryption
        98:95:36:35:98:51:26:92:66:c6:db:cd:ad:1a:a9:7f:12:2c:
        02:c3:36:28:4f:05:20:f3:85:a2:a1:f7:4d:6c:4b:68:47:0a:
        6f:f9:f3:6e:fa:e7:cf:cc:57:a5:7f:60:d6:d9:ba:7f:f3:81:
        16:e2:d7:c5:83:0c:1a:84:82:24:9a:ab:5f:20:5c:21:26:24:
        b7:6d:03:5f:ad:8e:10:9b:8c:2b:9a:6c:bc:a0:0c:4d:5c:52:
        d7:00:bb:ff:b9:73:aa:17:69:98:ca:a5:4c:79:bc:9e:73:48:
        b1:b5:c1:90:d8:88:89:f4:a2:55:bb:78:6b:e8:91:37:19:3f:
        37:7d:20:c4:ea:c1:f3:17:f1:4f:49:b5:6d:fe:f3:24:3b:f1:
        84:98:d0:0e:f4:24:bd:7e:e7:86:ee:6f:ff:7d:6c:49:fa:75:
        4d:d9:eb:f8:7c:1f:cd:3d:c3:16:33:23:38:8c:96:72:62:50:
        2d:6f:ea:68:0c:a6:ba:bb:0e:08:f5:5d:e9:c0:d2:c9:be:f3:
        ae:73:ae:63:ba:f6:8d:34:e9:60:b1:6e:a2:f8:cb:8b:fd:03:
        2c:c1:91:e0:45:12:e6:26:98:8a:51:16:6f:5c:36:20:6f:fd:
        99:96:3a:7b:8b:b1:56:2c:de:b7:91:ec:36:bc:14:56:c3:df:
        62:fd:d4:36
```

```
-----BEGIN CERTIFICATE-----
MIIF7zCCBNegAwIBAgIRANB9jBXAuny2RGmYseqJh58wDQYJKoZIhvcNAQEFBQAw
gewxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMREwDwYDVQQHEwhT
YW4gSm9zZTEdMBsGA1UEChMUQ2lzY28gU21hbGwgQnVzaW5lc3MxMzAxBgNVBAsT
KkNpc2NvIFNtYWxsIEJ1c2luZXNzIENlcnRpZmljYXRlIEF1dGhvcml0eTE1MDMG
A1UEAxMsQ2lzY28gU21hbGwgQnVzaW5lc3MgQ2xpZW50IFJvb3QgQXV0aG9yaXR5
IDIxKjAoBgkqhkiG9w0BCQEWG2Npc2Nvc2ItY2VydGFkbWluQGNpc2NvLmNvbTAe
Fw0xMzA4MDIyMjM3NDNaFw0zNTA2MjgyMjM3NDNaMIHsMQswCQYDVQQGEwJVUzET
```

FENpc2NvIFNtYWxsIEJ1c2luZXNzMTMwMQYDVQQLEypDaXNjbyBTbWFsbCBCdXNp
bmVzcyBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkxNTAzBgNVBAMTLENpc2NvIFNtYWxs
IEJ1c2luZXNzIENsaWVudCBSb290IEF1dGhvcml0eSAyMSowKAYJKoZIhvcNAQkB
FhtjaXNjb3NiLWNlcnRhZG1pbkBjaXNjby5jb20wggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQC/wvg65saJIYyCoHmRc3LzdNWoTqc9ewKrayyNcYICdnr6
vy6M57BHFZarg49IDefnFfLtVC7NfeM2NPbrBaPVOVcuau6yCrd7pt2C6WqUAS+J
HVKT9OwjCK5vBAqUXZKU1jrEWGnaKy5kz3cOKYLDvn166/j00VwYd4WkXugeUfbU
efHhyER8Z62c95uAdB8yBXnD1WdB3xyAmhBXgJt+q+ZQJIJCBs/fNH0K6XBW3G8K
xRsyevDhcy4h1JJ61lOWg7ONgrx/XgPt6X5jObs3CsYyx/7bP7CKAoWDeCqHMlqx
gv843w1LgzGOr3jmeUaUji7DGDQ2MZC2OokeBhpnAgMBAAGjggGIMIIBhDAdBgNV
HQ4EFgQU+MIzZ6kS/F1DI55V035XQBpVQhAwggErBgNVHSMEggEiMIIBHoAU+MIz
Z6kS/F1DI55V035XQBpVQhChgfKkge8wgewxCzAJBgNVBAYTAlVTMRMwEQYDVQQI
EwpDYWxpZm9ybmlhMREwDwYDVQQHEwhTYW4gSm9zZTEdMBsGA1UEChMUQ2lzY28g
U21hbGwgQnVzaW5lc3MxMzAxBgNVBAsTKkNpc2NvIFNtYWxsIEJ1c2luZXNzIENl
cnRpZmljYXRlIEF1dGhvcml0eTE1MDMGA1UEAxMsQ2lzY28gU21hbGwgQnVzaW5l
c3MgQ2xpZW50IFJvb3QgQXV0aG9yaXR5IDIxKjAoBgkqhkiG9w0BCQEWG2Npc2Nv
c2ItY2VydGFkbWluQGNpc2NvLmNvbYIRANB9jBXAuny2RGmYseqJh58wDAYDVR0T
BAUwAwEB/zARBglghkgBhvhCAQEEBAMCAgQwEwYDVR0lBAwwCgYIKwYBBQUHAwIw
DQYJKoZIhvcNAQEFBQADggEBAJiVNjWYUSaSZsbbza0aqX8SLALDNihPBSDzhaKh
901sS2hHCm/5827658/MV6V/YNbZun/zgRbi18WDDBqEgiSaq18gXCEmJLdtA1+t
jhCbjCuabLygDE1cUtcAu/+5c6oXaZjKpUx5vJ5zSLG1wZDYiIn0olW7eGvokTcZ
Pzd9IMTqwfMX8U9JtW3+8yQ78YSY0A70JL1+54bub/99bEn6dU3Z6/h8H809wxYz
IziMlnJiUC1v6mgMprq7Dgj1XenA0sm+865zrmO69o006WCxbqL4y4v9AyzBkeBF
EuYmmIpRFm9cNiBv/ZmWOnuLsVYs3reR7Da8FFbD32L91DY=
-----END CERTIFICATE-----

But you should not recognize me as the trusted source of such certificate ...

Despite of it, you may rate the response if it will help you ;-)

See More

Log in or register to post comments

robin.johnson@b... 5 years ago

The new certificates that are being issued by Cisco for Provisioning are issued by
issuer= /C=US/ST=California/L=San Jose/O=Cisco Small Business/OU=Cisco Small Business Certificate Authority/CN=Cisco Small Business Provisioning Root Authority 2/emailAddress=ciscosb-certadmin@cisco.com

Does anybody have a copy of that root, to make testing of provisioning easier? (specifically to have in the trusted CA's on my test code)

See More

Log in or register to post comments

robin.johnson@b... 5 years ago

I found it, with some digging.
Attached is: ca_crt.pem.txt, which is all of the CAs that seem to be on the device, with the x509 -text output added (by me).

It does correctly verify a certificate issued by the Provisioning Root Authority 2.

Attachment:
ca_crt.pem_.txt

Log in or register to post comments

Dan Lukes 5 years ago
★

The certificate you asked for is printed in the message just above your question.

Note that full bundle of root certificates is attached as combinedca-new.crt (or so) to every certificate you got signed from ciscosb-certadmin@cisco...

See More

Log in or register to post comments

robin.johnson@b... 5 years ago

The certificate you included is NOT the same as the one I was looking for.
Yours was "CN=Cisco Small Business Client Root Authority 2"

I wanted "CN=Cisco Small Business Provisioning Root Authority 2"

And Cisco at least as of the email I got yesterday from ciscosb-certadmin@ contained just my requested cert in a zipfile, and no other attachments. No CAs were included at all; hence my digging and attaching the CAs from the 7.5.6b firmware.

See More

Log in or register to post comments

Dan Lukes 5 years ago

★

```
The certificate you included is NOT the same as the one I was looking for.
```

True. Mea culpa. Sorry for it.

Log in or register to post comments

Dan Lukes 6 years ago

★

Note the older firmwares (exact list of them is not known, but it include even most recent firmware of PAP2T, pre-7.5.2b versions of SPA[35]0x firmware, ...) doesn't support SSL connection with Diffie-Hellman key larger than 1024b. As HTTP browsers are going to use larger keys by default, the affected devices will refuse connection to such kind of server with no helpful message in syslog.

So if HTTPS server is used for secure provisioning, it's configuration needs to be tuned accordingly.

Unfortunately, this issue is documented nowhere by Cisco.

Log in or register to post comments

This Document

Follow | Shortcut | Abuse | PDF

Related Content

RTP on SIP TRUNK | CUCM--->SIP TRUNK---->2911VGW(SIP TRUNK)---->ITSP

Lakshman Singh | 122 views

How Cisco detects RTP packages?

hofo123456 | 66 views

No audio on incoming call with CFA, CME, SIP trunk

alig.norbert | 221 views

Porting Dell L3 Config to 3560-X

Brian Maxwell | 47 views

Porting Dell L3 Config to 3560-X

Brian Maxwell | 15 views