



Cynthia

@cynthia@blahaj.social

Have you ever wanted to check your own public IP address without having to bother with HTTPS?

Now you can get it by just looking at the server certificate if you connect to `emudhra.insecureoldshit.com:443`!

It will even indicate if your are using SNI, so convenient!

All of this thanks to a CA finally implementing the XKCD 221 specification.

```
root@cyntest: ~  
$ openssl s_client -connect emudhra.insecureoldshit.com:443 -servername googl  
e.com -showcerts < /dev/null | openssl x509 -subject -noout  
Connecting to 2a01:4f9:c01d:bef::1  
depth=3 C=IN, OU=emSign PKI, O=eMudhra Technologies Limited, CN=emSign ECC Ro  
ot CA - G3  
verify return:1  
depth=2 C=IN, O=eMudhra Technologies Limited, CN=emSign Root TLS CA - G3  
verify return:1  
depth=1 C=US, O=eMudhra Inc, CN=EM OV TLS CA - G3C  
verify return:1  
depth=0 C=AQ, O=Penguin Association, OU=You, CN=[2a01:4f9:c015:1a9c::1]:57792  
verify return:1  
DONE  
subject=C=AQ, O=Penguin Association, OU=You, CN=[2a01:4f9:c015:1a9c::1]:57792  
$
```

Oct 21, 2026, 12:53 AM · · Web

5 boosts · 0 quotes · 12 favorites



Cynthia

@cynthia

9h

Here's a second picture actually showing the SNI (it will put whatever the server name is into a DNS SAN).

Search

Trending

Live feeds

About

Mastodon is the best way to keep up with what's happening.

Follow anyone across the fediverse and see it all in chronological order. No algorithms, ads, or clickbait in sight.

Create account

Login

```
Connecting to 2a01:4f9:c01d:bef::1
depth=3 C=IN, OU=emSign PKI, O=eMudhra Technologies Limited, CN=emSign
ot CA - G3
verify return:1
depth=2 C=IN, O=eMudhra Technologies Limited, CN=emSign Root TLS CA - G3
verify return:1
depth=1 C=US, O=eMudhra Inc, CN=EM OV TLS CA - G3C
verify return:1
depth=0 C=AQ, O=Penguin Association, OU=You, CN=[2a01:4f9:c015:1a9c::1]:38806
verify return:1
DONE
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 0 (0x0)
    Signature Algorithm: ecdsa-with-SHA384
    Issuer: C=US, O=eMudhra Inc, CN=EM OV TLS CA - G3C
    Validity
      Not Before: Oct 20 22:54:35 2026 GMT
      Not After : Oct 20 22:55:05 2026 GMT
    Subject: C=AQ, O=Penguin Association, OU=You, CN=[2a01:4f9:c015:1a9c:
:1]:38806
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
      Public-Key: (256 bit)
      pub:
        04:95:61:11:86:61:1c:97:dd:0f:b5:e3:75:9b:07:
        81:72:6a:b7:8a:f6:03:83:7f:c2:62:70:c9:01:07:
        48:ea:a0:b0:5a:39:52:a8:cf:33:b5:d6:50:07:43:
        b4:26:72:52:8e:4e:f0:df:6a:8d:d7:71:a4:84:3b:
        0b:32:27:18:10
      ASN1 OID: prime256v1
      NIST CURVE: P-256
    X509v3 extensions:
      X509v3 Authority Key Identifier:
        34:EA:EA:0C:EB:C9:0A:DA:F9:D0:C5:E2:ED:9B:78:C9:87:9E:1B:6C
      X509v3 Subject Alternative Name:
        DNS:eXample.com, DNS:*.google.com, IP Address
:2A01:4F9:C015:1A9C:0:0:0:1
      Signature Algorithm: ecdsa-with-SHA384
      Signature Value:
        30:66:02:31:00:c3:b8:72:24:c3:25:2f:b7:dd:e5:08:c4:9a:
        79:87:c8:ac:5f:c4:b8:3c:c1:c5:cb:19:fb:d2:e9:a8:fc:be:
        63:17:3c:d4:37:b6:24:68:35:0f:d5:a4:e0:bf:49:a2:b7:02:
        31:00:87:ce:74:a0:3d:5f:7c:29:d2:6a:2c:13:92:d9:43:fe:
        20:db:e9:93:21:47:32:29:40:4b:9c:2e:d9:06:34:4c:42:f5:
        19:1e:97:e2:59:bd:62:16:06:f4:18:c0:0c:65
```

Hide



Trending

Live feeds

About

Mastodon is the best way to keep up with what's happening.

Follow anyone across the fediverse and see it all in chronological order. No algorithms, ads, or clickbait in sight.

Create account

Login

0



Stéphane Bortzmeyer

@bortzmeyer@mastodon.gougere.fr

1h

@cynthia subject `CN=[2a01:e34:CENSORED]:44642,OU=You,O=Penguin Association,C=AQ

I love the country 😊

1



Cynthia

@cynthia

1h

@bortzmeyer My go to whenever I need a country code :)

0





Cley Faye

@CleyFaye@mastodon.top

1h

@cynthia Some people see a big issue, other sees an opportunity :D



Trending

Live feeds

About

Mastodon is the best way to keep up with what's happening.

Follow anyone across the fediverse and see it all in chronological order. No algorithms, ads, or clickbait in sight.

Create account

Login