Cryptography in the Wild (Public Key Infrastructure, Certificates)

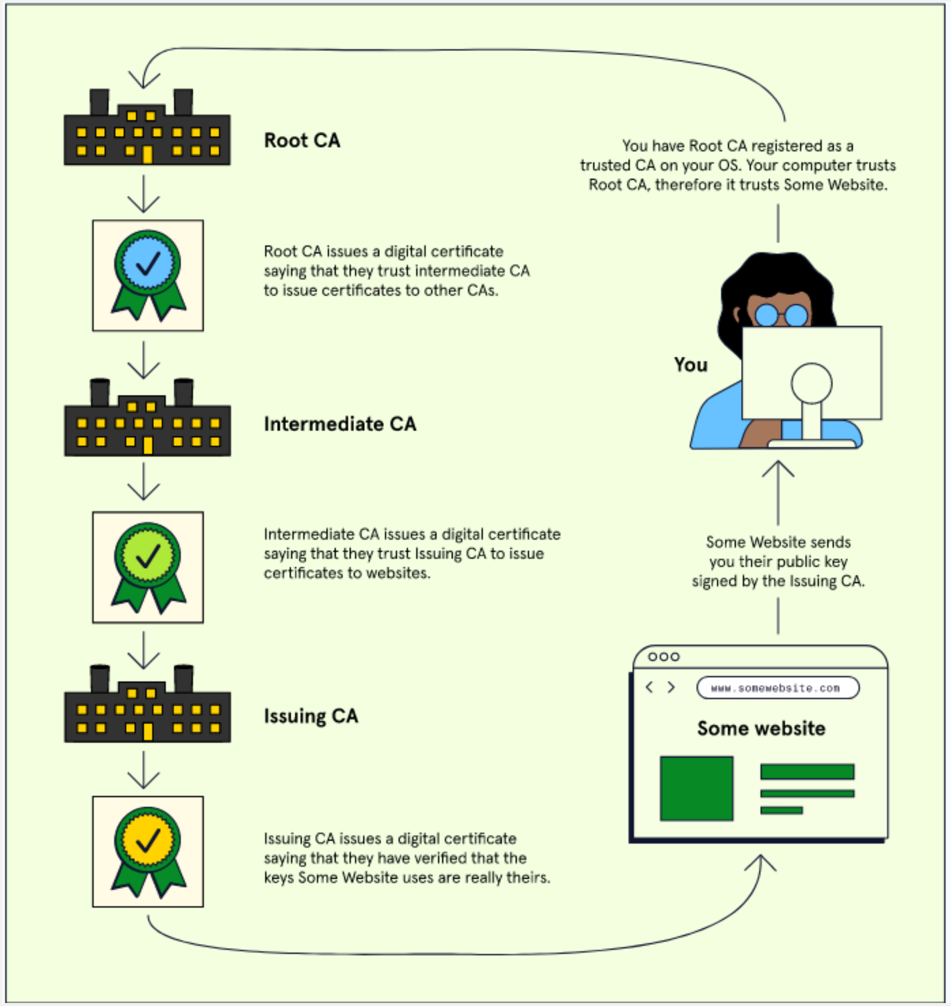
Index

- What is PKI?
- How does Browser do it?
- Handshake and trust?!
- How do it get this Certificate?
- CA and End devices.
- Types of Certificates.
- Cert Examples.
- Demo.
- SSL Cert Security.
- SSH Certificate.
- DNSSEC.
- Q n A.
- Reference.

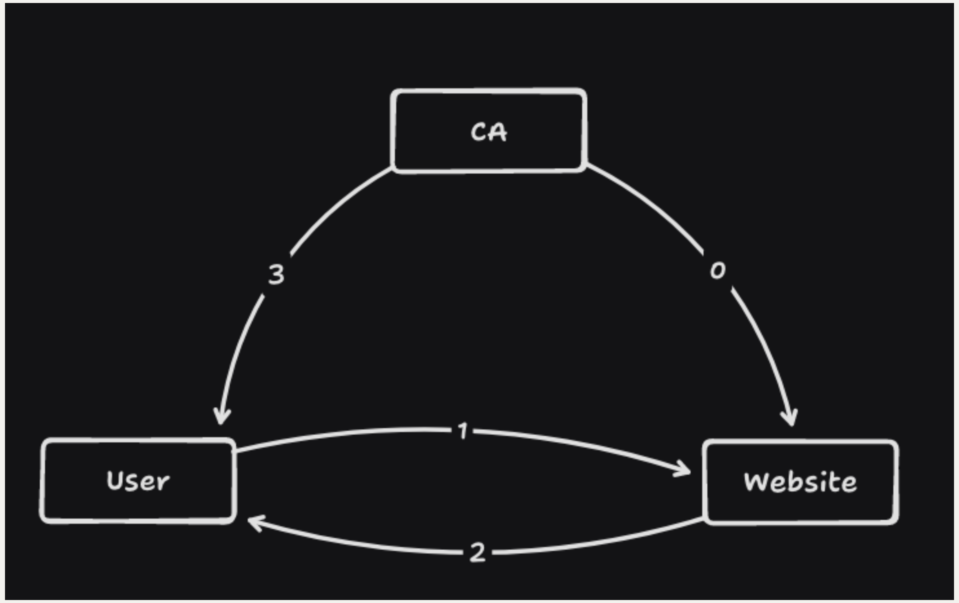
What is PKI?

- A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.[Wikipedia]
- Its most notable applications are HTTPS.
- PKI is mostly used in TLS/SSL to secure connections.
- Digital certificates with X.509 standards (will look at it later).[2]
- Digital Certificates are issued by Certificate Authorities(Digicerts, GLobalSign, LetsEncrypt, Comodo, GoDaddy, Etc) .

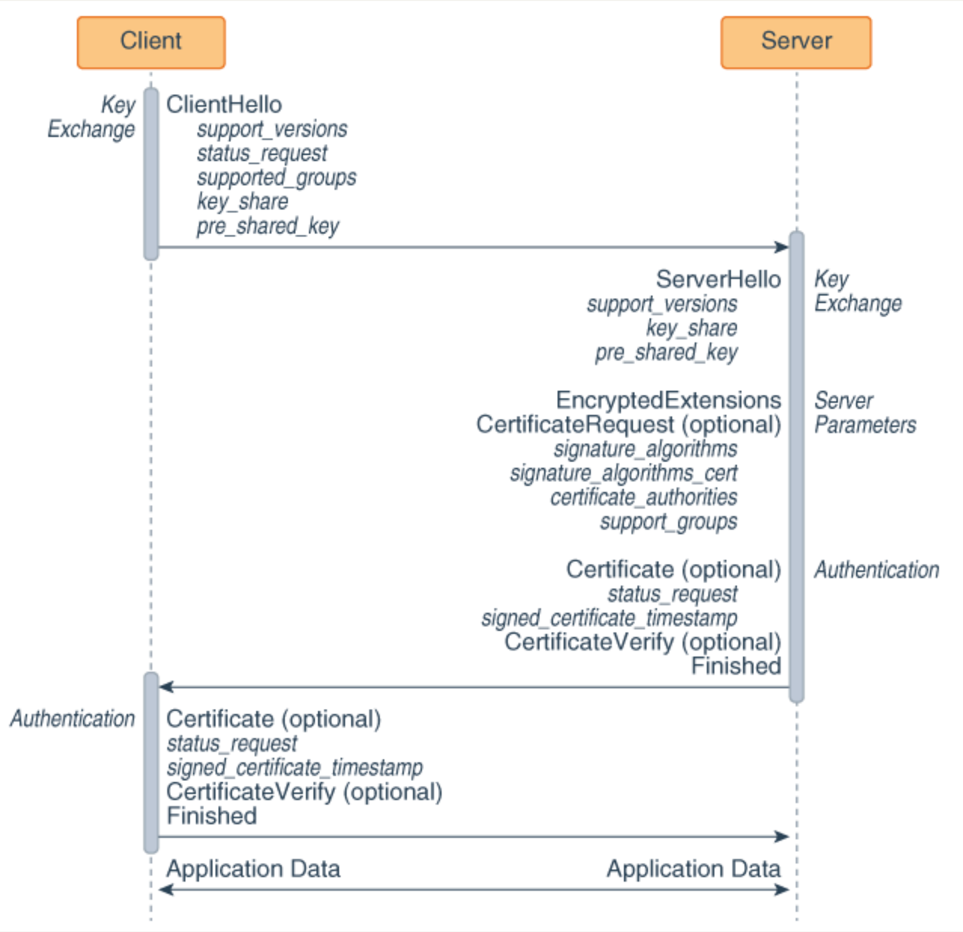
How does Browser do it?



Root CA
You have Root CA registered as a trusted CA on your OS. Your computer trusts Root CA, therefore it trusts Some Website.
Root CA issues a digital certificate saying that they trust intermediate CA to issue certificates to other CAs.
You
Intermediate CA
Intermediate CA issues a digital certificate saying that they trust Issuing CA to issue certificates to websites.
Some Website sends you their public key signed by the Issuing CA.
www.somewebsite.com
Some website
Issuing CA
Issuing CA issues a digital certificate saying that they have verified that the keys Some Website uses are really theirs.



Handshake and Trust ?!



Client

Server

Key Exchange

ClientHello
support_versions
status_request
supported_groups
key_share
pre_shared_key

ServerHello
support_versions
key_share
pre_shared_key

Key Exchange

EncryptedExtensions
CertificateRequest (optional)
signature_algorithms
signature_algorithms_cert
certificate_authorities
support_groups

Server Parameters

Certificate (optional)
status_request
signed_certificate_timestamp
CertificateVerify (optional)
Finished

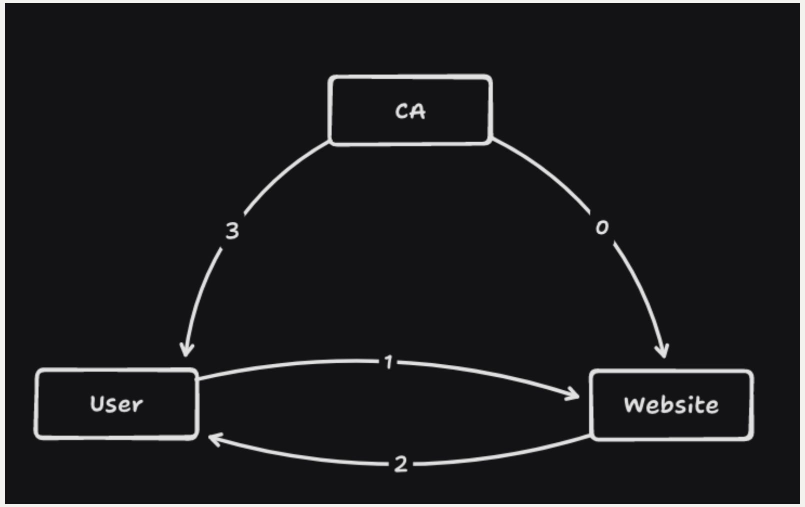
Authentication

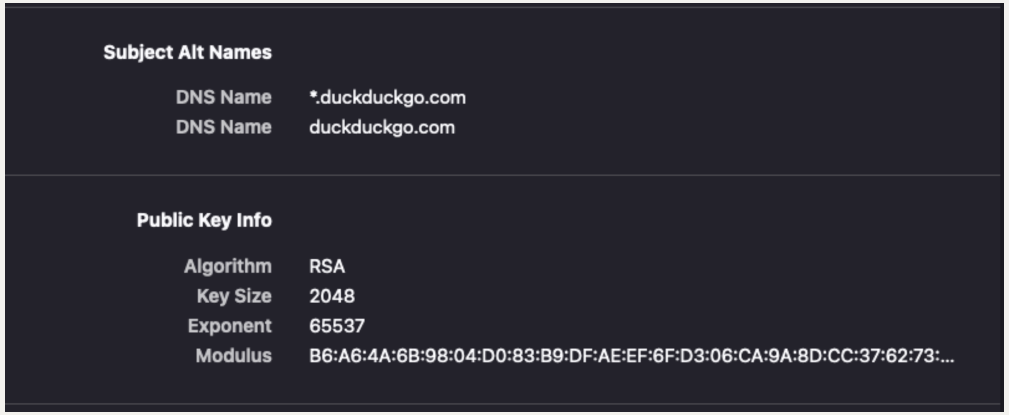
Authentication

Certificate (optional)
status_request
signed_certificate_timestamp
CertificateVerify (optional)
Finished

Application Data

Application Data





Subject Alt Names

DNS Name	*.duckduckgo.com
DNS Name	duckduckgo.com

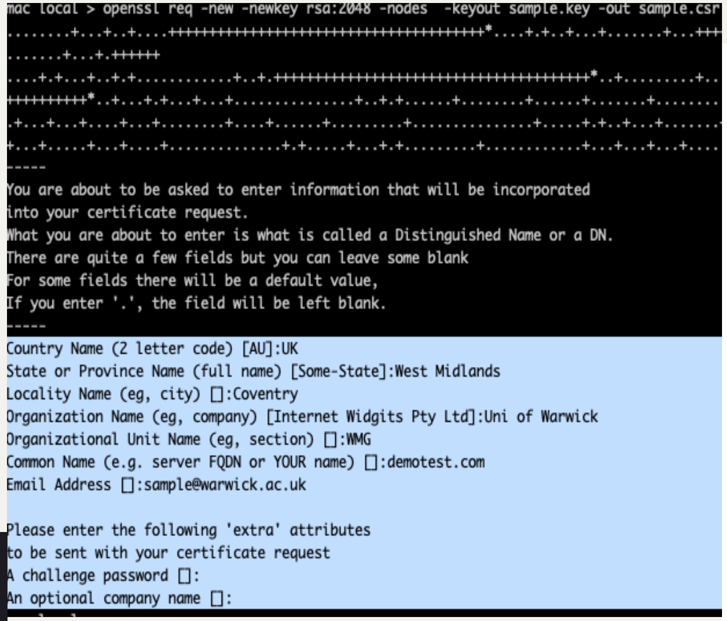
Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	B6:A6:4A:6B:98:04:D0:83:B9:DF:AE:EF:6F:D3:06:CA:9A:8D:CC:37:62:73:...

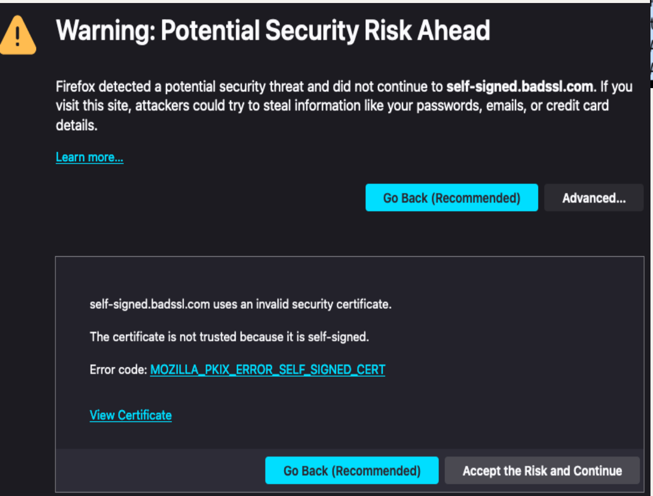
TLS 1.3

How do it get this Certificate?

- Need a webserver, domain, CSR(certificate signing request) and a CA.
- Can use a local, but need a well established one for public and browsers.



```
mac local > openssl req -new -newkey rsa:2048 -nodes  -keyout sample.key -out sample.csr
........+...+..+....+++++++++++++++++++++++++++++++++++++++*....+.+..+...+.......+...+++
.......+...+.++++++
....+.+...+..+.+...........+..+.+++++++++++++++++++++++++++++++++++++++*..+.........+..
++++++++++*..+...+.+...+...+..............+..+.+......+........+......+.......+.......
.+...+...+....+...+.......+....+......+.........+..............+.....+.+..+...+.......
+...+.....+...+....+............+.+.....+...+.+.........+...........+...+...+...+....
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:UK
State or Province Name (full name) [Some-State]:West Midlands
Locality Name (eg, city) []:Coventry
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Uni of Warwick
Organizational Unit Name (eg, section) []:WMG
Common Name (e.g. server FQDN or YOUR name) []:demotest.com
Email Address []:sample@warwick.ac.uk

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```



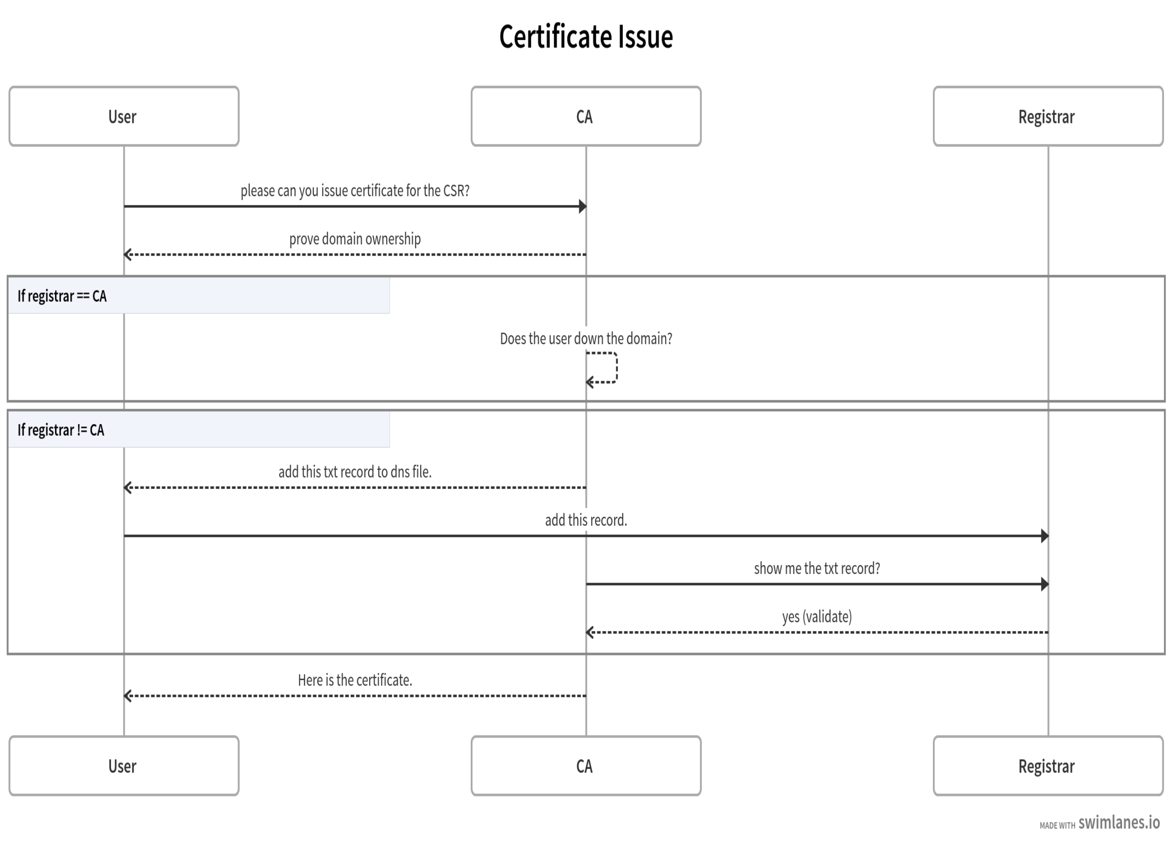
Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **self-signed.badssl.com**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

self-signed.badssl.com uses an invalid security certificate.

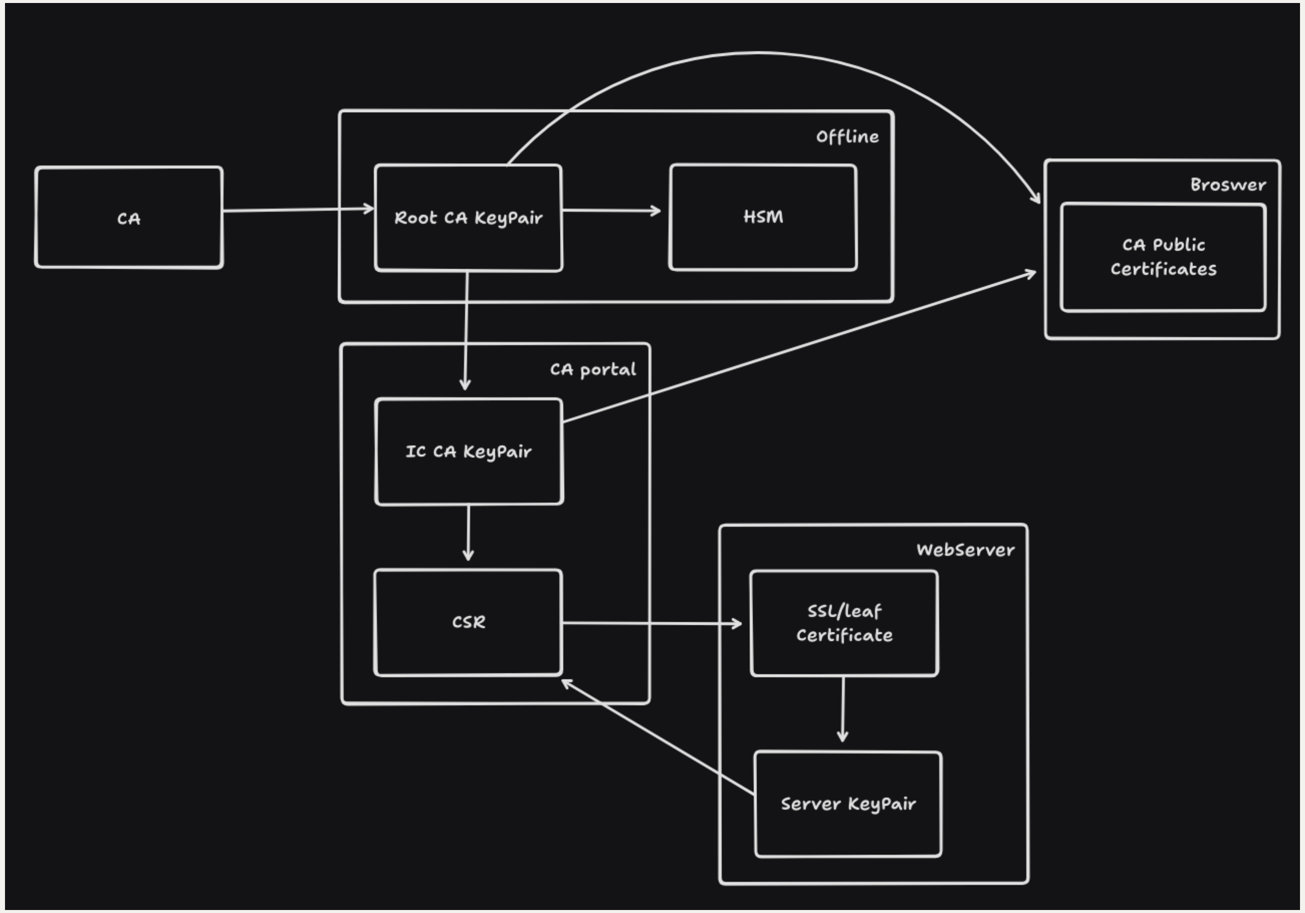
The certificate is not trusted because it is self-signed.

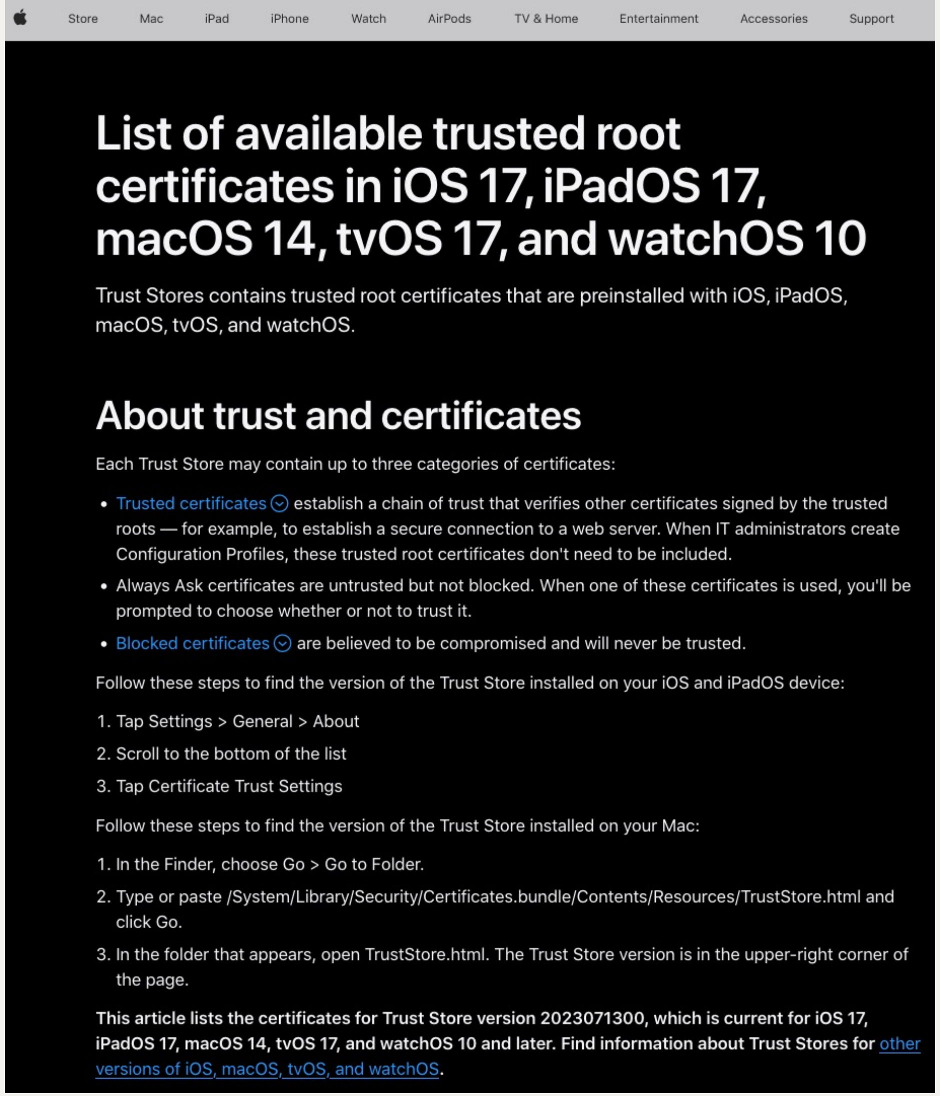
Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT



Certificate Issue

CA and End devices





List of available trusted root certificates in iOS 17, iPadOS 17, macOS 14, tvOS 17, and watchOS 10

Trust Stores contains trusted root certificates that are preinstalled with iOS, iPadOS, macOS, tvOS, and watchOS.

About trust and certificates

Each Trust Store may contain up to three categories of certificates:

- Trusted certificates establish a chain of trust that verifies other certificates signed by the trusted roots — for example, to establish a secure connection to a web server. When IT administrators create Configuration Profiles, these trusted root certificates don't need to be included.
- Always Ask certificates are untrusted but not blocked. When one of these certificates is used, you'll be prompted to choose whether or not to trust it.
- Blocked certificates are believed to be compromised and will never be trusted.

Follow these steps to find the version of the Trust Store installed on your iOS and iPadOS device:

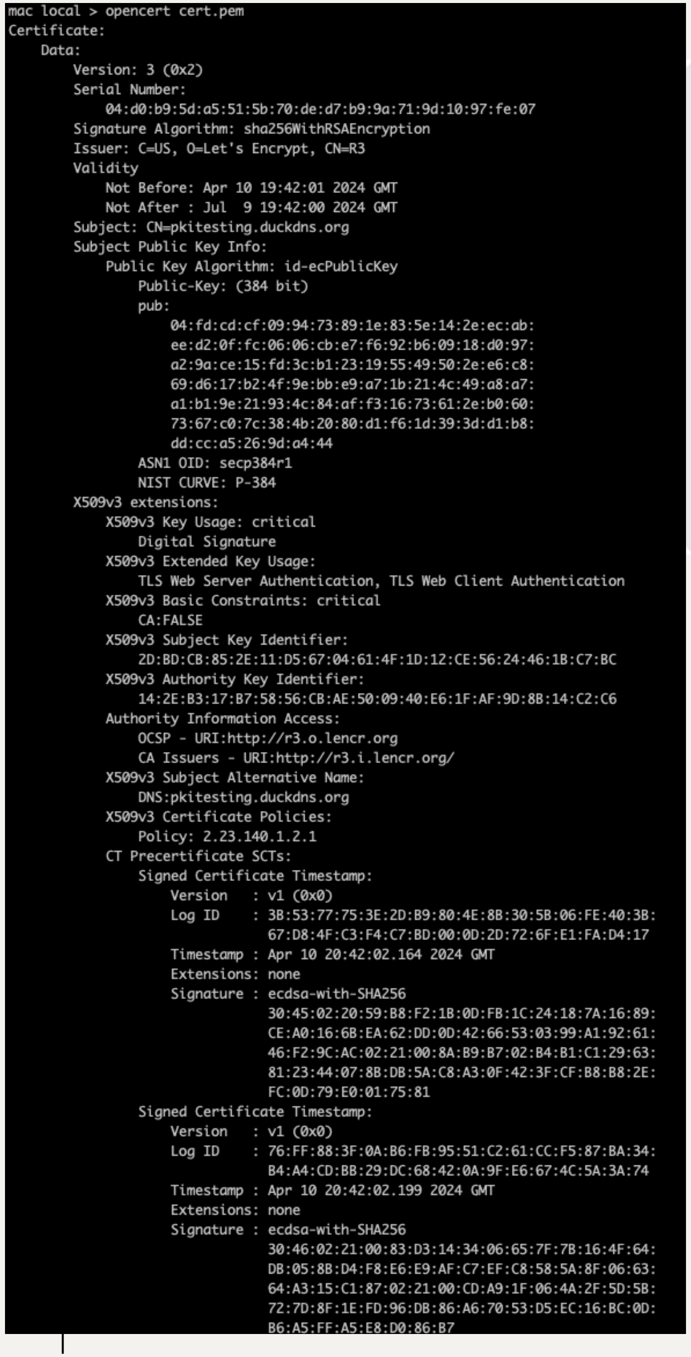
1. Tap Settings > General > About
2. Scroll to the bottom of the list
3. Tap Certificate Trust Settings

Follow these steps to find the version of the Trust Store installed on your Mac:

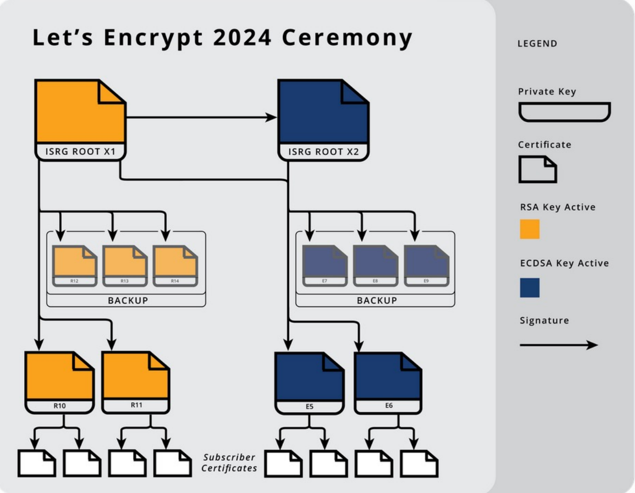
1. In the Finder, choose Go > Go to Folder.
2. Type or paste /System/Library/Security/Certificates.bundle/Contents/Resources/TrustStore.html and click Go.
3. In the folder that appears, open TrustStore.html. The Trust Store version is in the upper-right corner of the page.

This article lists the certificates for Trust Store version 2023071300, which is current for iOS 17, iPadOS 17, macOS 14, tvOS 17, and watchOS 10 and later. Find information about Trust Stores for other versions of iOS, macOS, tvOS, and watchOS.

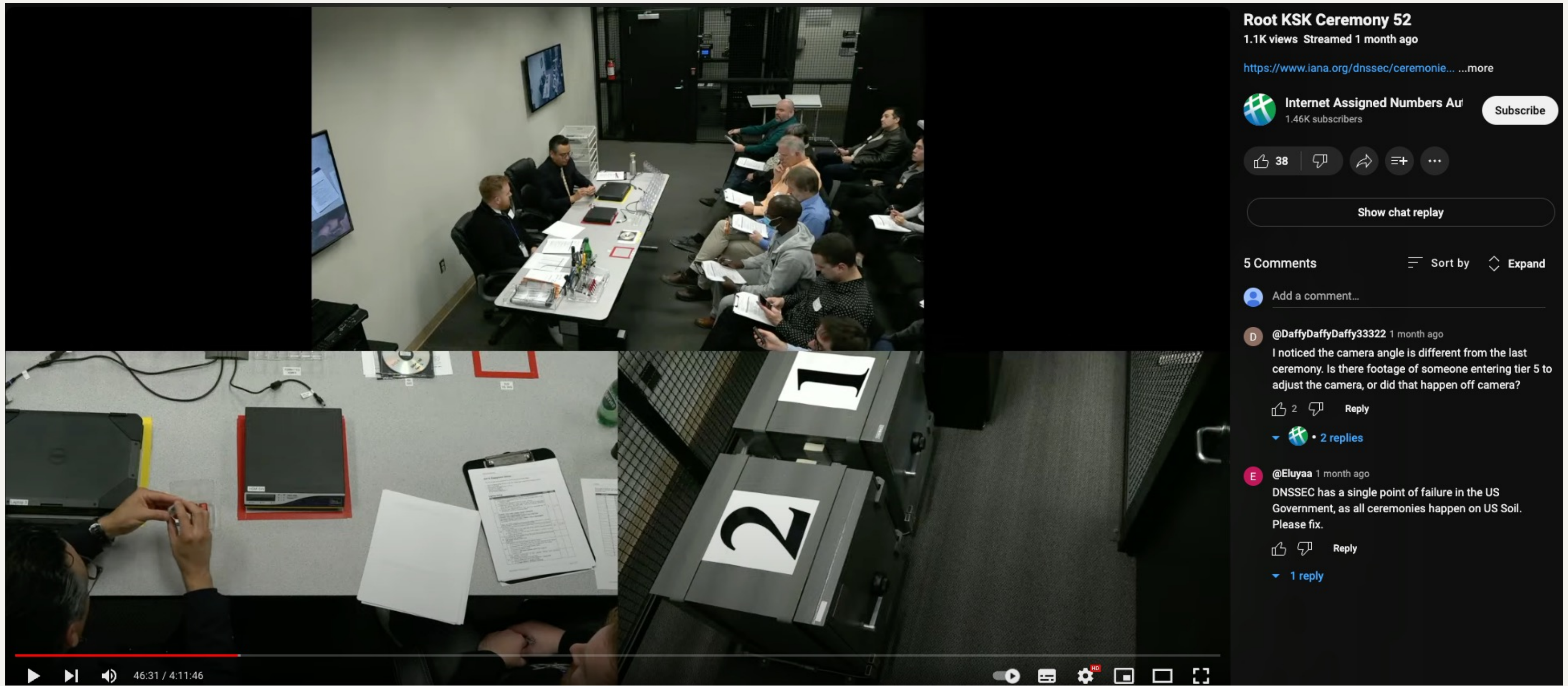
Browser CAs[3-5]



```
mac local > opencert cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:d0:b9:5d:a5:51:5b:70:de:d7:b9:9a:71:9d:10:97:fe:07
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Let's Encrypt, CN=R3
        Validity
            Not Before: Apr 10 19:42:01 2024 GMT
            Not After : Jul  9 19:42:00 2024 GMT
        Subject: CN=pkitesting.duckdns.org
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:fd:cd:cf:09:94:73:89:1e:83:5e:14:2e:ec:ab:
                    ee:d2:0f:fc:06:06:cb:e7:f6:92:b6:09:18:d0:97:
                    a2:9a:ce:15:fd:3c:b1:23:19:55:49:50:2e:e6:c8:
                    69:d6:17:b2:4f:9e:bb:e9:a7:1b:21:4c:49:a8:a7:
                    a1:b1:9e:21:93:4c:84:af:f3:16:73:61:2e:b0:60:
                    73:67:c0:7c:38:4b:20:80:d1:f6:1d:39:3d:d1:b8:
                    dd:cc:a5:26:9d:a4:44
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Key Identifier:
                2D:BD:CB:85:2E:11:D5:67:04:61:4F:1D:12:CE:56:24:46:1B:C7:BC
            X509v3 Authority Key Identifier:
                14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6
            Authority Information Access:
                OCSP - URI:http://r3.o.lencr.org
                CA Issuers - URI:http://r3.i.lencr.org/
            X509v3 Subject Alternative Name:
                DNS:pkitesting.duckdns.org
            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.1
            CT Precertificate SCTs:
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : 3B:53:77:75:3E:2D:B9:80:4E:8B:30:5B:06:FE:40:3B:
                                67:D8:4F:C3:F4:C7:BD:00:0D:2D:72:6F:E1:FA:D4:17
                    Timestamp : Apr 10 20:42:02.164 2024 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:45:02:20:59:B8:F2:1B:0D:FB:1C:24:18:7A:16:89:
                                CE:A0:16:6B:EA:62:DD:0D:42:66:53:03:99:A1:92:61:
                                46:F2:9C:AC:02:21:00:8A:B9:B7:02:B4:B1:C1:29:63:
                                81:23:44:07:8B:DB:5A:C8:A3:0F:42:3F:CF:B8:B8:2E:
                                FC:0D:79:E0:01:75:81
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : 76:FF:88:3F:0A:B6:FB:95:51:C2:61:CC:F5:87:BA:34:
                                B4:A4:CD:BB:29:DC:68:42:0A:9F:E6:67:4C:5A:3A:74
                    Timestamp : Apr 10 20:42:02.199 2024 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:46:02:21:00:83:D3:14:34:06:65:7F:7B:16:4F:64:
                                DB:05:8B:D4:F8:E6:E9:AF:C7:EF:C8:58:5A:8F:06:63:
                                64:A3:15:C1:87:02:21:00:CD:A9:1F:06:4A:2F:5D:5B:
                                72:7D:8F:1E:FD:96:DB:86:A6:70:53:D5:EC:16:BC:0D:
                                B6:A5:FF:A5:E8:D0:86:B7
```



Let's Encrypt 2024 Ceremony



Root KSK Ceremony 52
1.1K views Streamed 1 month ago

https://www.iana.org/dnssec/ceremonie... ...more

Internet Assigned Numbers Au
1.46K subscribers

5 Comments

@DaffyDaffyDaffy33322 1 month ago
I noticed the camera angle is different from the last ceremony. Is there footage of someone entering tier 5 to adjust the camera, or did that happen off camera?

@Eluyaa 1 month ago
DNSSEC has a single point of failure in the US Government, as all ceremonies happen on US Soil. Please fix.

Types of Certificates

Domain validated certificates(DV)

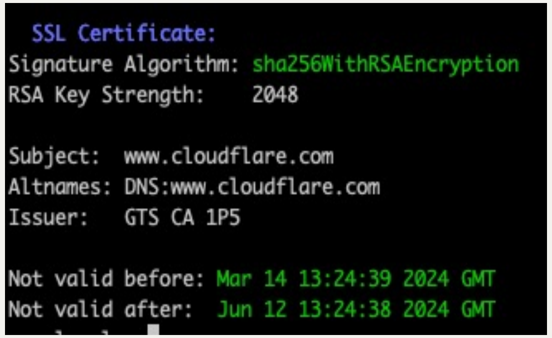
- Single certificate.
- Multi-domain(SAN- subject alternative name) certificate.
- Wildcard certificate- ***Big No No*** covers lots of subdomains.

Fancy Certificates

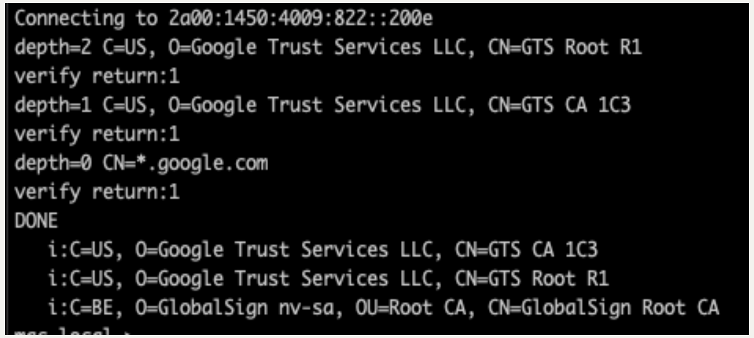
- Organisation validated certificate(OV).
- Extended validated certificate(EV).

Godaddy product(No), good resource: https://www.godaddy.com/en-uk/web-security/ssl-certificate

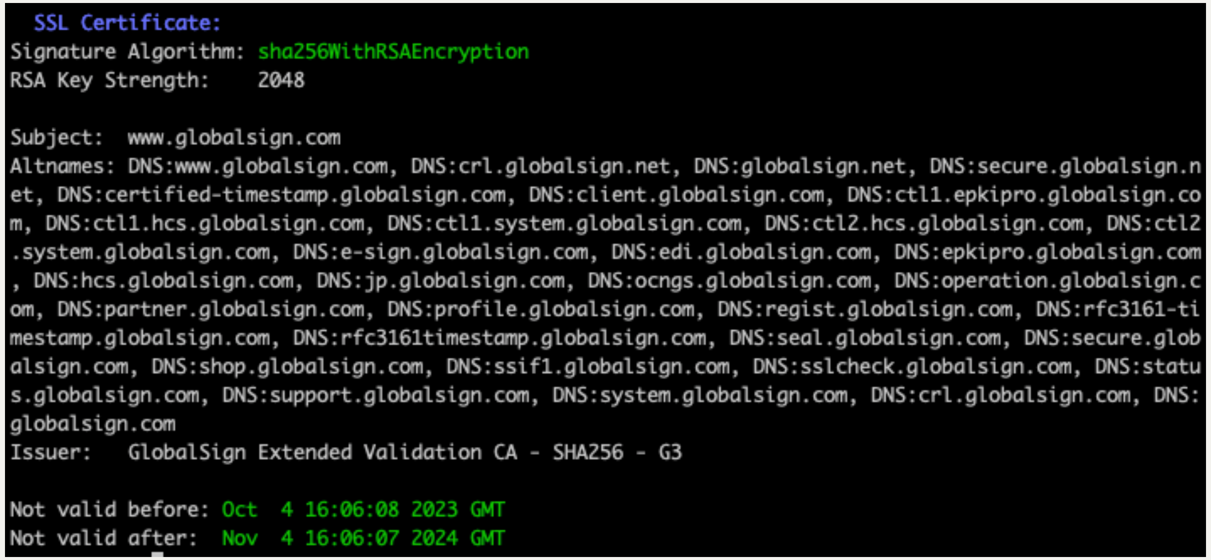
Cert Examples



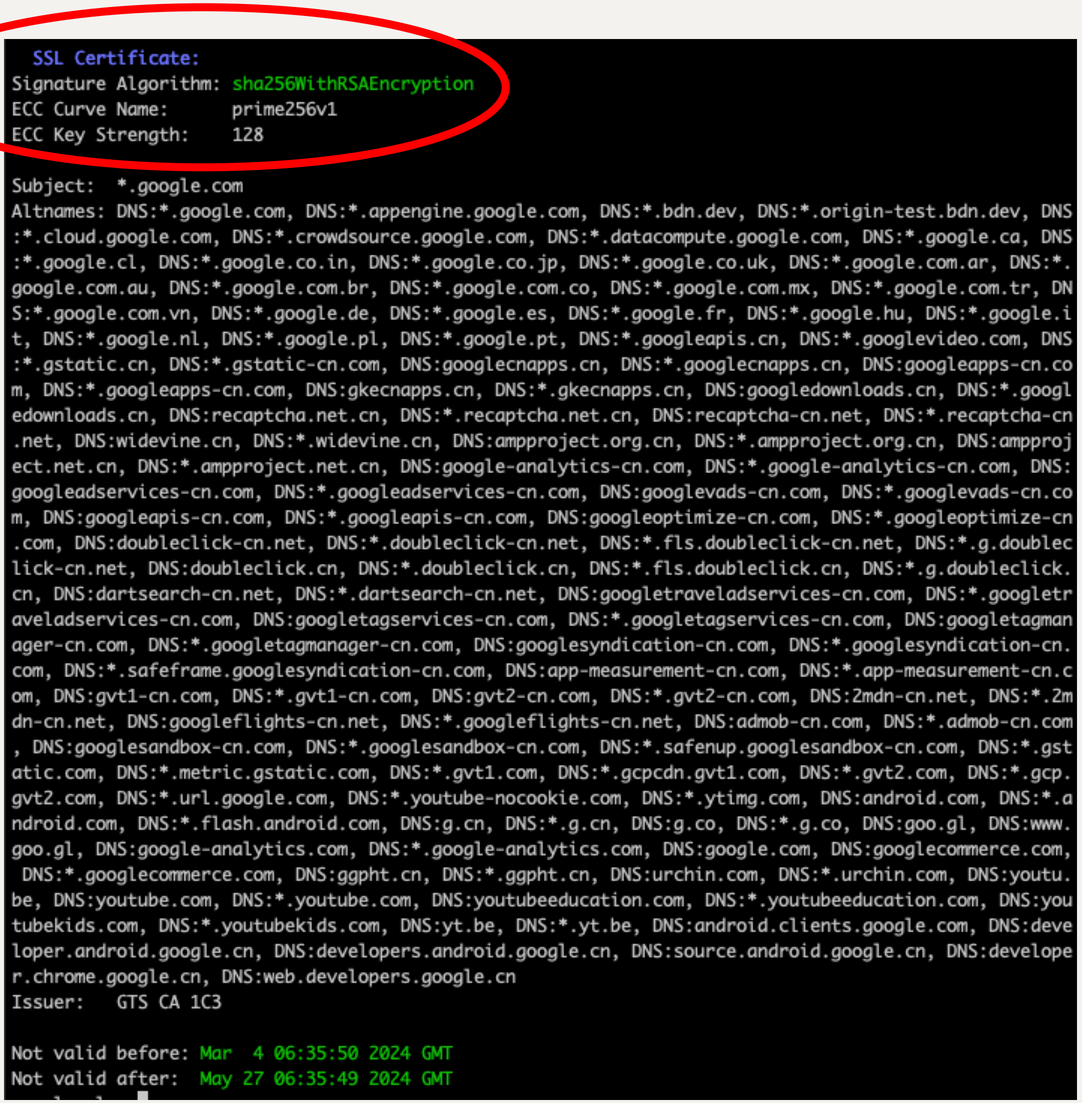
```
  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  www.cloudflare.com
Altnames: DNS:www.cloudflare.com
Issuer:   GTS CA 1P5

Not valid before: Mar 14 13:24:39 2024 GMT
Not valid after:  Jun 12 13:24:38 2024 GMT
```



```
Connecting to 2a00:1450:4009:822::200e
depth=2 C=US, O=Google Trust Services LLC, CN=GTS Root R1
verify return:1
depth=1 C=US, O=Google Trust Services LLC, CN=GTS CA 1C3
verify return:1
depth=0 CN=*.google.com
verify return:1
DONE
   i:C=US, O=Google Trust Services LLC, CN=GTS CA 1C3
   i:C=US, O=Google Trust Services LLC, CN=GTS Root R1
   i:C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign Root CA
```



```
  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  www.globalsign.com
Altnames: DNS:www.globalsign.com, DNS:crl.globalsign.net, DNS:globalsign.net, DNS:secure.globalsign.n
et, DNS:certified-timestamp.globalsign.com, DNS:client.globalsign.com, DNS:ctl1.epkipro.globalsign.co
m, DNS:ctl1.hcs.globalsign.com, DNS:ctl1.system.globalsign.com, DNS:ctl2.hcs.globalsign.com, DNS:ctl2
.system.globalsign.com, DNS:e-sign.globalsign.com, DNS:edi.globalsign.com, DNS:epkipro.globalsign.com
, DNS:hcs.globalsign.com, DNS:jp.globalsign.com, DNS:ocngs.globalsign.com, DNS:operation.globalsign.c
om, DNS:partner.globalsign.com, DNS:profile.globalsign.com, DNS:regist.globalsign.com, DNS:rfc3161-ti
mestamp.globalsign.com, DNS:rfc3161timestamp.globalsign.com, DNS:seal.globalsign.com, DNS:secure.glob
alsign.com, DNS:shop.globalsign.com, DNS:ssif1.globalsign.com, DNS:sslcheck.globalsign.com, DNS:statu
s.globalsign.com, DNS:support.globalsign.com, DNS:system.globalsign.com, DNS:crl.globalsign.com, DNS:
globalsign.com
Issuer:   GlobalSign Extended Validation CA - SHA256 - G3

Not valid before: Oct  4 16:06:08 2023 GMT
Not valid after:  Nov  4 16:06:07 2024 GMT
```



```
  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
ECC Curve Name:      prime256v1
ECC Key Strength:    128

Subject:  *.google.com
Altnames: DNS:*.google.com, DNS:*.appengine.google.com, DNS:*.bdn.dev, DNS:*.origin-test.bdn.dev, DNS
:*.cloud.google.com, DNS:*.crowdsource.google.com, DNS:*.datacompute.google.com, DNS:*.google.ca, DNS
:*.google.cl, DNS:*.google.co.in, DNS:*.google.co.jp, DNS:*.google.co.uk, DNS:*.google.com.ar, DNS:*.
google.com.au, DNS:*.google.com.br, DNS:*.google.com.co, DNS:*.google.com.mx, DNS:*.google.com.tr, DN
S:*.google.com.vn, DNS:*.google.de, DNS:*.google.es, DNS:*.google.fr, DNS:*.google.hu, DNS:*.google.i
t, DNS:*.google.nl, DNS:*.google.pl, DNS:*.google.pt, DNS:*.googleapis.cn, DNS:*.googlevideo.com, DNS
:*.gstatic.cn, DNS:*.gstatic-cn.com, DNS:googlecnapps.cn, DNS:*.googlecnapps.cn, DNS:googleapps-cn.co
m, DNS:*.googleapps-cn.com, DNS:gkecnapps.cn, DNS:*.gkecnapps.cn, DNS:googledownloads.cn, DNS:*.googl
edownloads.cn, DNS:recaptcha.net.cn, DNS:*.recaptcha.net.cn, DNS:recaptcha-cn.net, DNS:*.recaptcha-cn
.net, DNS:widevine.cn, DNS:*.widevine.cn, DNS:ampproject.org.cn, DNS:*.ampproject.org.cn, DNS:ampproj
ect.net.cn, DNS:*.ampproject.net.cn, DNS:google-analytics-cn.com, DNS:*.google-analytics-cn.com, DNS:
googleadservices-cn.com, DNS:*.googleadservices-cn.com, DNS:googlevads-cn.com, DNS:*.googlevads-cn.co
m, DNS:googleapis-cn.com, DNS:*.googleapis-cn.com, DNS:googleoptimize-cn.com, DNS:*.googleoptimize-cn
.com, DNS:doubleclick-cn.net, DNS:*.doubleclick-cn.net, DNS:*.fls.doubleclick-cn.net, DNS:*.g.doublec
lick-cn.net, DNS:doubleclick.cn, DNS:*.doubleclick.cn, DNS:*.fls.doubleclick.cn, DNS:*.g.doubleclick.
cn, DNS:dartsearch-cn.net, DNS:*.dartsearch-cn.net, DNS:googletraveladservices-cn.com, DNS:*.googletr
aveladservices-cn.com, DNS:googletagservices-cn.com, DNS:*.googletagservices-cn.com, DNS:googletagman
ager-cn.com, DNS:*.googletagmanager-cn.com, DNS:googlesyndication-cn.com, DNS:*.googlesyndication-cn.
com, DNS:*.safeframe.googlesyndication-cn.com, DNS:app-measurement-cn.com, DNS:*.app-measurement-cn.c
om, DNS:gvt1-cn.com, DNS:*.gvt1-cn.com, DNS:gvt2-cn.com, DNS:*.gvt2-cn.com, DNS:2mdn-cn.net, DNS:*.2m
dn-cn.net, DNS:googleflights-cn.net, DNS:*.googleflights-cn.net, DNS:admob-cn.com, DNS:*.admob-cn.com
, DNS:googlesandbox-cn.com, DNS:*.googlesandbox-cn.com, DNS:*.safenup.googlesandbox-cn.com, DNS:*.gst
atic.com, DNS:*.metric.gstatic.com, DNS:*.gvt1.com, DNS:*.gcpcdn.gvt1.com, DNS:*.gvt2.com, DNS:*.gcp.
gvt2.com, DNS:*.url.google.com, DNS:*.youtube-nocookie.com, DNS:*.ytimg.com, DNS:android.com, DNS:*.a
ndroid.com, DNS:*.flash.android.com, DNS:g.cn, DNS:*.g.cn, DNS:g.co, DNS:*.g.co, DNS:goo.gl, DNS:www.
goo.gl, DNS:google-analytics.com, DNS:*.google-analytics.com, DNS:google.com, DNS:googlecommerce.com,
 DNS:*.googlecommerce.com, DNS:ggpht.cn, DNS:*.ggpht.cn, DNS:urchin.com, DNS:*.urchin.com, DNS:youtu.
be, DNS:youtube.com, DNS:*.youtube.com, DNS:youtubeeducation.com, DNS:*.youtubeeducation.com, DNS:you
tubekids.com, DNS:*.youtubekids.com, DNS:yt.be, DNS:*.yt.be, DNS:android.clients.google.com, DNS:deve
loper.android.google.cn, DNS:developers.android.google.cn, DNS:source.android.google.cn, DNS:develope
r.chrome.google.cn, DNS:web.developers.google.cn
Issuer:   GTS CA 1C3

Not valid before: Mar  4 06:35:50 2024 GMT
Not valid after:  May 27 06:35:49 2024 GMT
```

Demo

Nginx Proxy Server:

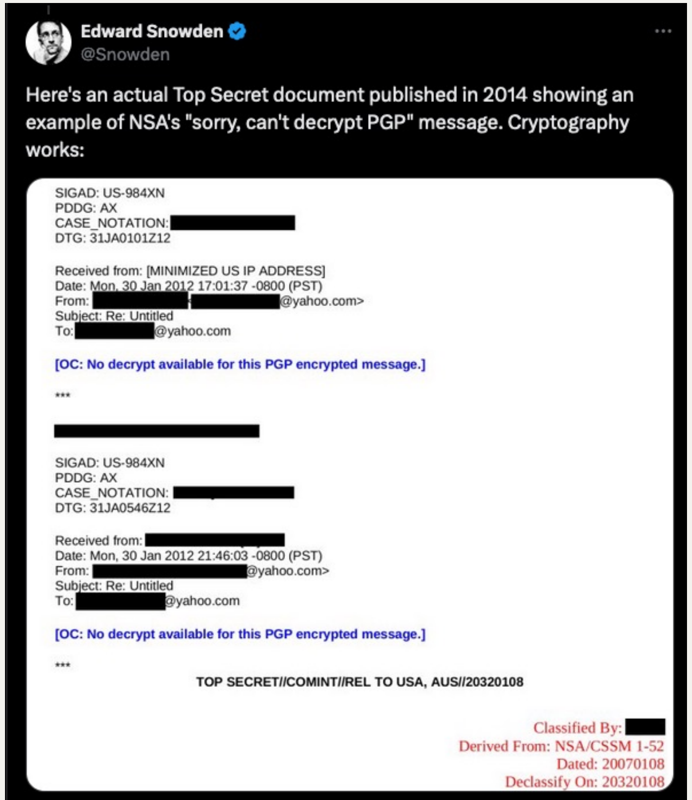
- Get the certificate from LetsEncrypt.
- Apply to one of the proxy localhosts.

Docker containers.

- Nginx Configuration.
- Issued certificates and details (x.509). ECC

SSL Cert Security

- Configuration issues[7].
- Test SSL for domains(https://ssltools.godaddy.com/views/certChecker) google.com, cert chain.
- Industry recommended Algorithm and Keysize. RSA (2048 or 3072 bits) ECDSA (Curves P-256 or P-384).
- SSL/TLS Inspection [8]. Rarely outside of Enterprise (Netskope One SASE, Palo Alto Networks Pan-OS).
- Trusted/Reputed CAs, going back to the CA trusted by the browsers.



Edward Snowden
@Snowden

Here's an actual Top Secret document published in 2014 showing an example of NSA's "sorry, can't decrypt PGP" message. Cryptography works:

SIGAD: US-984XN
PDDG: AX
CASE_NOTATION: [redacted]
DTG: 31JA0101Z12

Received from: [MINIMIZED US IP ADDRESS]
Date: Mon, 30 Jan 2012 17:01:37 -0800 (PST)
From: [redacted] [redacted]@yahoo.com>
Subject: Re: Untitled
To: [redacted]@yahoo.com

[OC: No decrypt available for this PGP encrypted message.]

***

[redacted]

SIGAD: US-984XN
PDDG: AX
CASE_NOTATION: [redacted]
DTG: 31JA0546Z12

Received from: [redacted]
Date: Mon, 30 Jan 2012 21:46:03 -0800 (PST)
From: [redacted]@yahoo.com>
Subject: Re: Untitled
To: [redacted]@yahoo.com

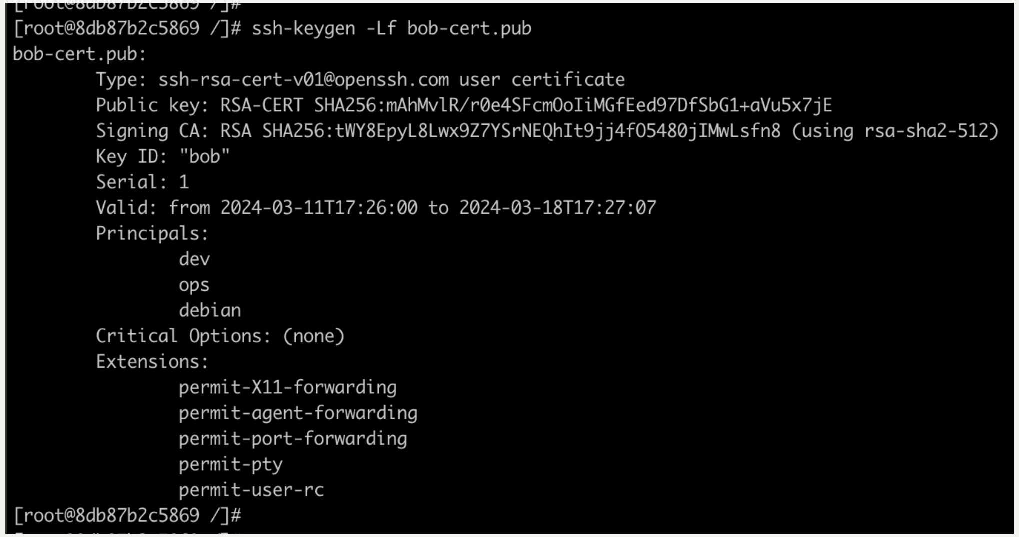
[OC: No decrypt available for this PGP encrypted message.]

***

TOP SECRET//COMINT//REL TO USA, AUS//20320108

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

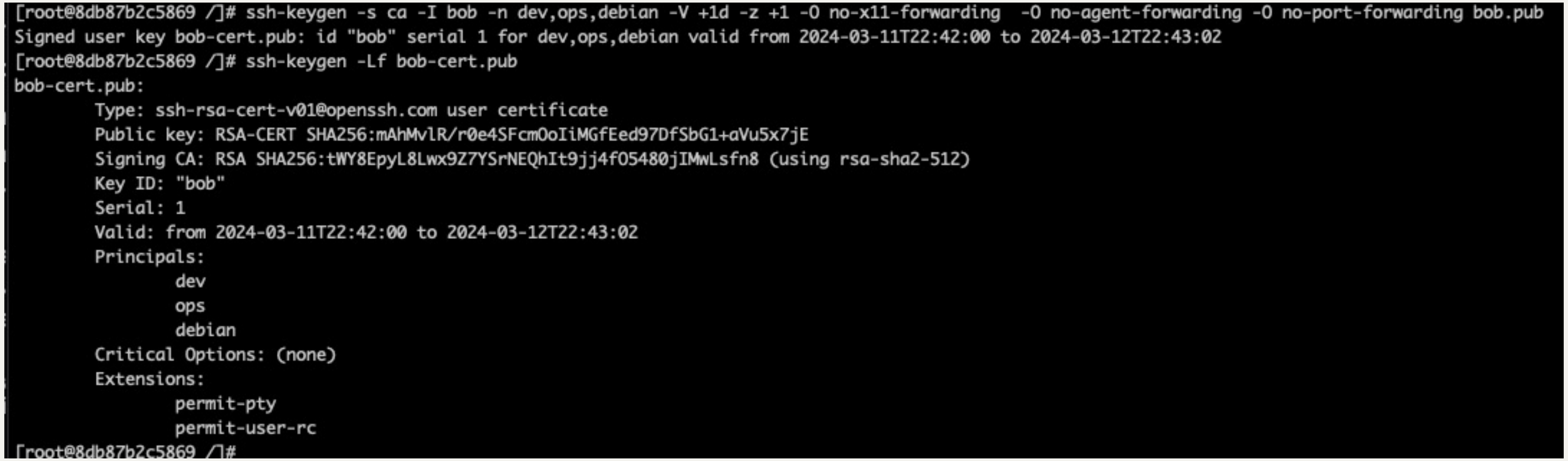
SSH Certificate



```
[root@8db87b2c5869 /]#
[root@8db87b2c5869 /]# ssh-keygen -Lf bob-cert.pub
bob-cert.pub:
        Type: ssh-rsa-cert-v01@openssh.com user certificate
        Public key: RSA-CERT SHA256:mAhMvlR/r0e4SFcmOoIiMGfEed97DfSbG1+aVu5x7jE
        Signing CA: RSA SHA256:tWY8EpyL8Lwx9Z7YSrNEQhIt9jj4f05480jIMwLsfn8 (using rsa-sha2-512)
        Key ID: "bob"
        Serial: 1
        Valid: from 2024-03-11T17:26:00 to 2024-03-18T17:27:07
        Principals:
                dev
                ops
                debian
        Critical Options: (none)
        Extensions:
                permit-X11-forwarding
                permit-agent-forwarding
                permit-port-forwarding
                permit-pty
                permit-user-rc
[root@8db87b2c5869 /]#
```

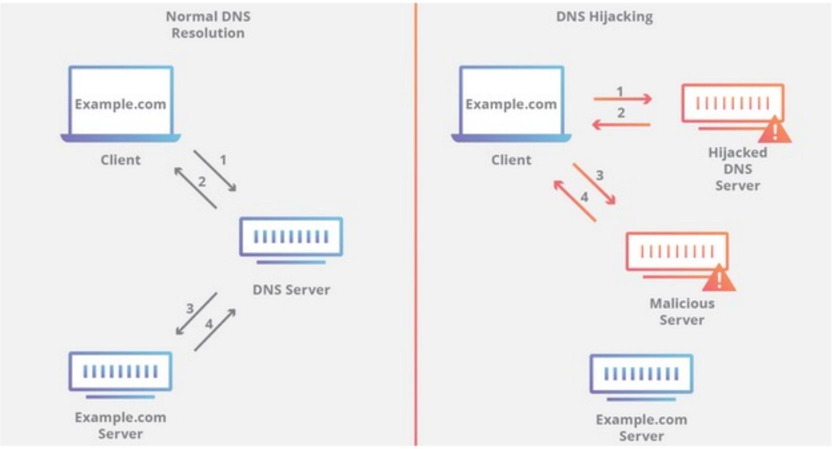
Lots of access

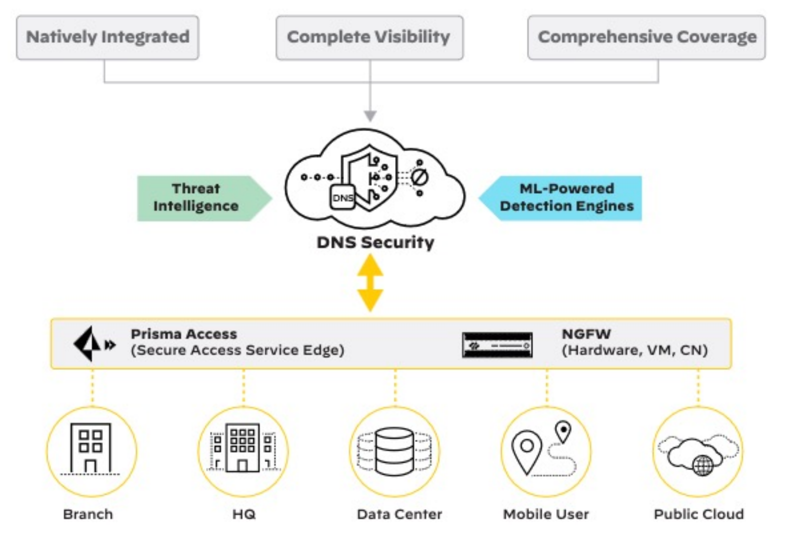
Limited access

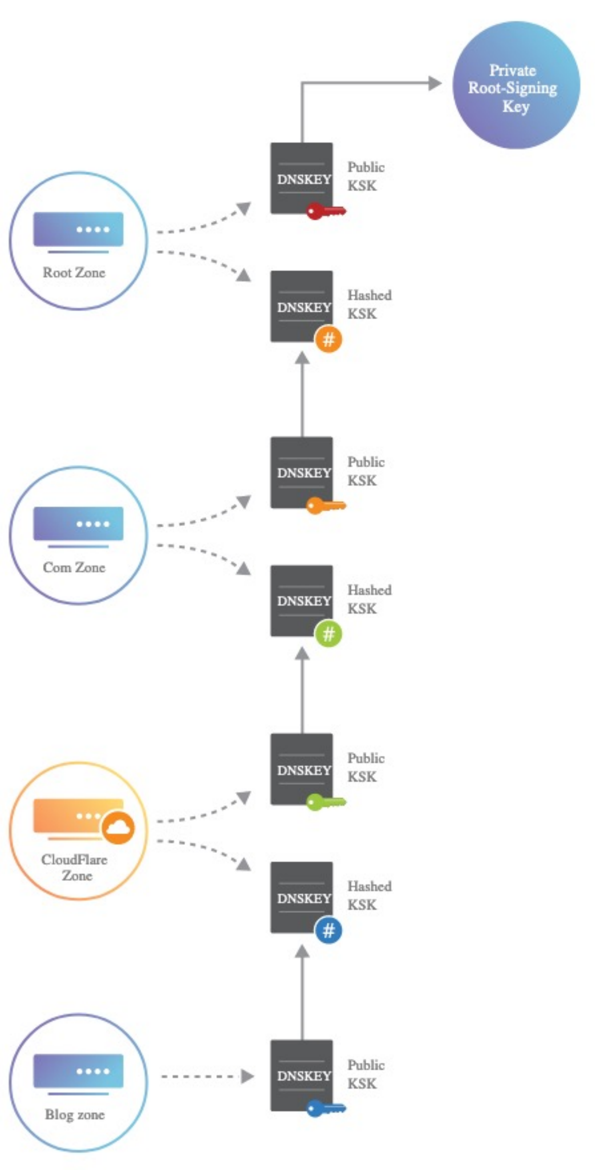


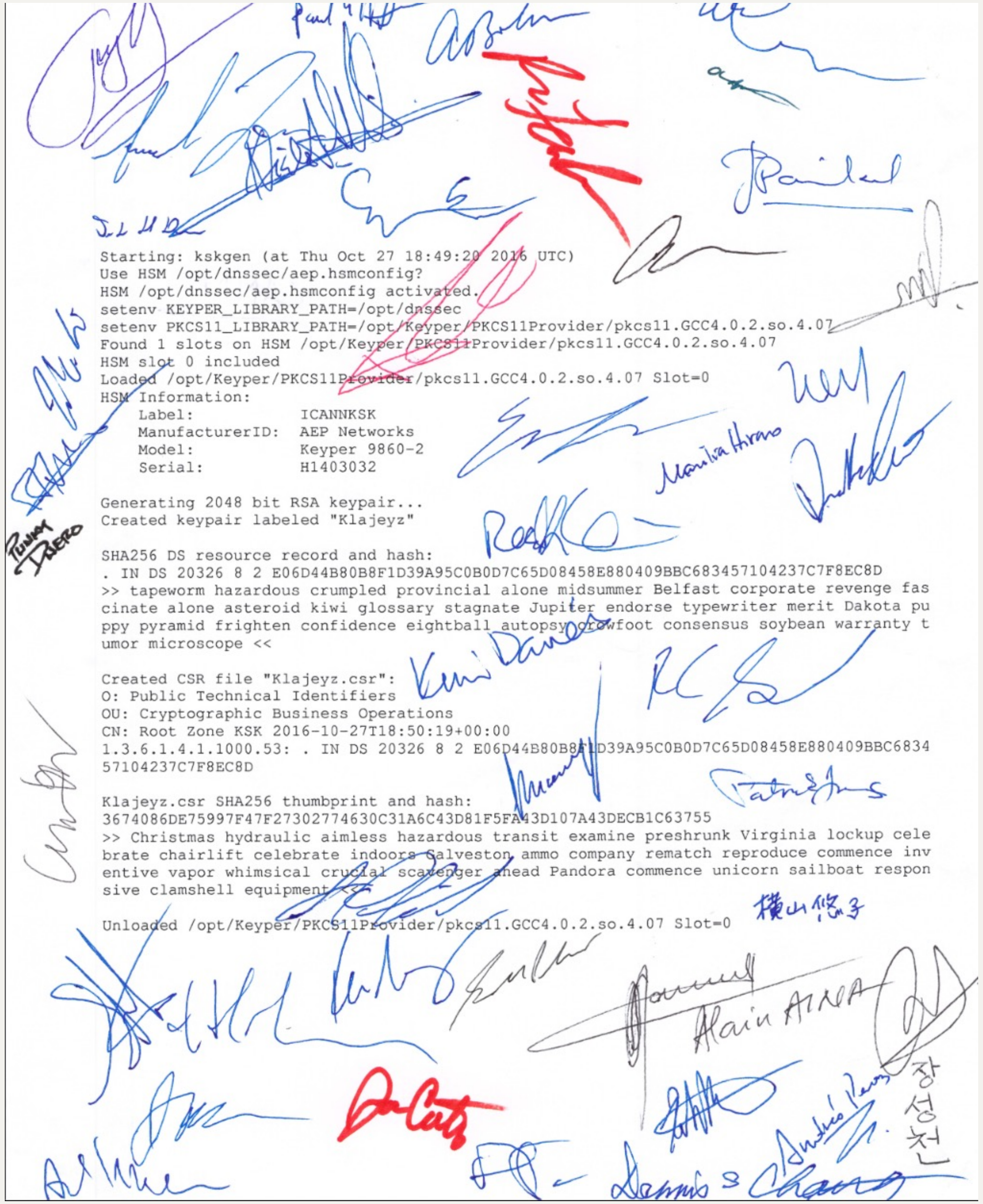
```
[root@8db87b2c5869 /]# ssh-keygen -s ca -I bob -n dev,ops,debian -V +1d -z +1 -O no-x11-forwarding  -O no-agent-forwarding -O no-port-forwarding bob.pub
Signed user key bob-cert.pub: id "bob" serial 1 for dev,ops,debian valid from 2024-03-11T22:42:00 to 2024-03-12T22:43:02
[root@8db87b2c5869 /]# ssh-keygen -Lf bob-cert.pub
bob-cert.pub:
        Type: ssh-rsa-cert-v01@openssh.com user certificate
        Public key: RSA-CERT SHA256:mAhMvlR/r0e4SFcmOoIiMGfEed97DfSbG1+aVu5x7jE
        Signing CA: RSA SHA256:tWY8EpyL8Lwx9Z7YSrNEQhIt9jj4f05480jIMwLsfn8 (using rsa-sha2-512)
        Key ID: "bob"
        Serial: 1
        Valid: from 2024-03-11T22:42:00 to 2024-03-12T22:43:02
        Principals:
                dev
                ops
                debian
        Critical Options: (none)
        Extensions:
                permit-pty
                permit-user-rc
[root@8db87b2c5869 /]#
```

DNSSEC







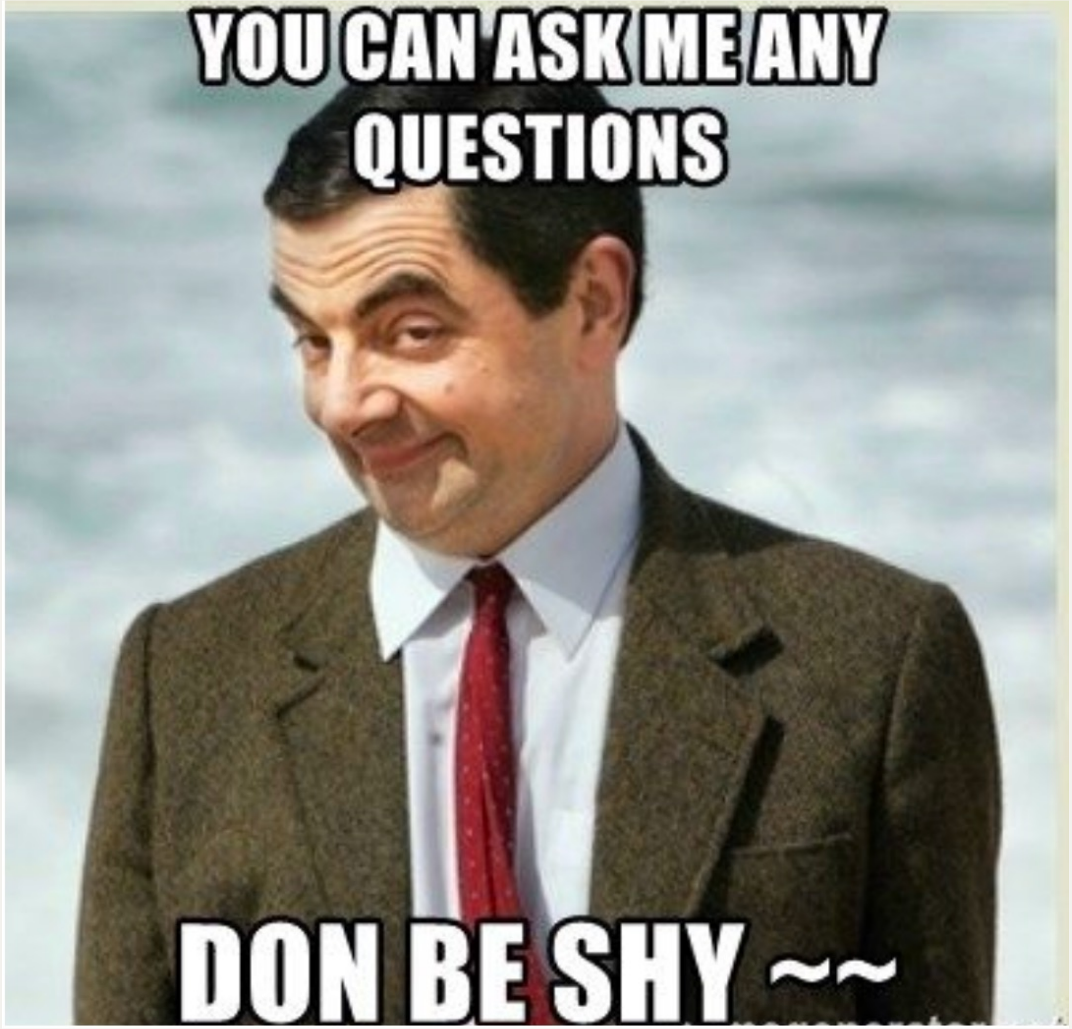


```
Starting: kskgen (at Thu Oct 27 18:49:20 2016 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:            ICANNKSK
    ManufacturerID:   AEP Networks
    Model:            Keyper 9860-2
    Serial:           H1403032

Generating 2048 bit RSA keypair...
Created keypair labeled "Klajeyz"

SHA256 DS resource record and hash:
. IN DS 20326 8 2 E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D
>> tapeworm hazardous crumpled provincial alone midsummer Belfast corporate revenge fas
cinate alone asteroid kiwi glossary stagnate Jupiter endorse typewriter merit Dakota pu
ppy pyramid frighten confidence eightball autopsy crowfoot consensus soybean warranty t
umor microscope <<

Created CSR file "Klajeyz.csr":
O: Public Technical Identifiers
OU: Cryptographic Business Operations
CN: Root Zone KSK 2016-10-27T18:50:19+00:00
1.3.6.1.4.1.1000.53: . IN DS 20326 8 2 E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC6834
57104237C7F8EC8D

Klajeyz.csr SHA256 thumbprint and hash:
3674086DE75997F47F27302774630C31A6C43D81F5FA43D107A43DECB1C63755
>> Christmas hydraulic aimless hazardous transit examine preshrunk Virginia lockup cele
brate chairlift celebrate indoors Galveston ammo company rematch reproduce commence inv
entive vapor whimsical crucial scavenger ahead Pandora commence unicorn sailboat respon
sive clamshell equipment <<

Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```

横山悠子

Alain AINA

THANK YOU FOR LISTENING
ANY QUESTIONS?


YOU CAN ASK ME ANY QUESTIONS
DON BE SHY ~~

Reference

1. https://pkic.org/
2. https://en.wikipedia.org/wiki/X.509
3. https://security.stackexchange.com/questions/49006/list-of-certificate-authorities-in-browsers-and-mobile-platforms
4. https://wiki.mozilla.org/CA/Included_Certificates
5. https://www.chromium.org/Home/chromium-security/root-ca-policy/
6. Root KSK Ceremony 52 (https://www.youtube.com/live/uiHzbIL3R6s?si=1hDiMqbxDtCCmn2h)
7. https://uk.godaddy.com/help/install-my-ssl-certificate-16623
8. https://www.ise.io/casestudies/fighting-back-against-ssl-inspection-or-how-ssl-should-work/