CYBER SECURITY LAB 7

Write the steps to check and analyze the browser and website digital certificates

What is digital certificates :

A **digital certificate** is like a **digital ID card** (think passport, driver’s license, or company ID) that:

1. **Identifies a website** (e.g., confirms you're really visiting `yourdomain.com`).
2. **Secures communication** using encryption (via public and private keys).

You can recognize websites using digital certificates by the **padlock icon** and `https://` in the browser address bar.

Contents of a X.509 certificate

The contents of a digital certificate typically include the following:

- **Information about the subject a.k.a. Subject Name** - "subject" refers to the site represented by the cert.
- **Information about the certificate issuer/certificate authority (CA)** - The CA is the body that issued and signed the certificate. More about this shortly
- **Serial number** - this is the serial number assigned by the issuer to this certificate. Each issuer must make sure each certificate it issues has a unique serial number.
- **Version** - the X.509 version used by a given certificate. These days, you'll usually find version 3.
- **Validity period** - certs aren't meant to last forever. The validity period defines the period over which the cert can still be deemed trustworthy.
- **Signature** - This is the **digital signature** of the entire digital certificate, generated using the certificate issuer's private key
- **Signature algorithm** - The cryptographic signature algorithm used to generate the digital signature (e.g. SHA-1 with RSA Encryption)
- **Public key information** - Information about the subject's public key. This includes:
    - the algorithm (e.g. Elliptic Curve Public Key),
    - the key size (e.g. 256 bits),
    - the key usage (e.g. can encrypt, verify, derive), and
    - the public key itself

Certificate Authority (CA)

□ Before your browser (Chrome, Firefox, Safari, etc.) connects to a website via **HTTPS**, it already has a set of **CA certificates**.

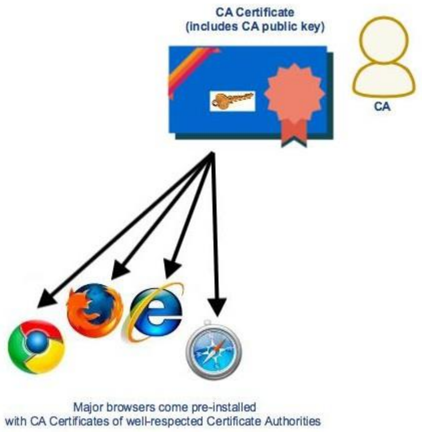
□ These are called **Certificate Authority (CA) certificates**.

□ Each CA certificate contains the **public key** of a trusted **CA** (like DigiCert, Sectigo, etc.).

□ When a website sends its **server certificate**, the browser uses the CA’s **public key** to:

- **Verify the digital signature**
- Make sure the website is **trusted and safe**

□ That’s why you don’t need to manually install anything—**browsers already have trusted CA certificates built in**.

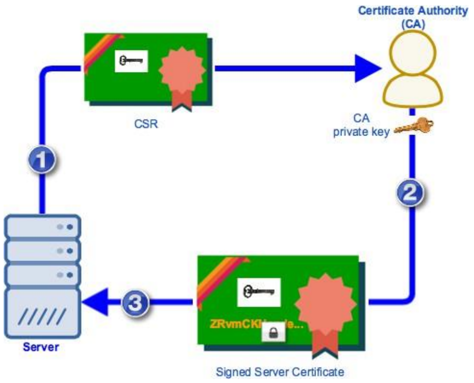

CA Certificate
(includes CA public key)
CA
Major browsers come pre-installed
with CA Certificates of well-respected Certificate Authorities

Generating CSRs and having your certificate signed by a CA

1. You generate a private key / public key pair and submit a CSR to a Certificate Authority. The contents of the CSR will form part of the final server certificate.

2. The CA verifies whether the certificate's information is correct and signs it using its (the CA's) private key. It then returns the signed server certificate to you.

3. You import the signed server certificate into your server.

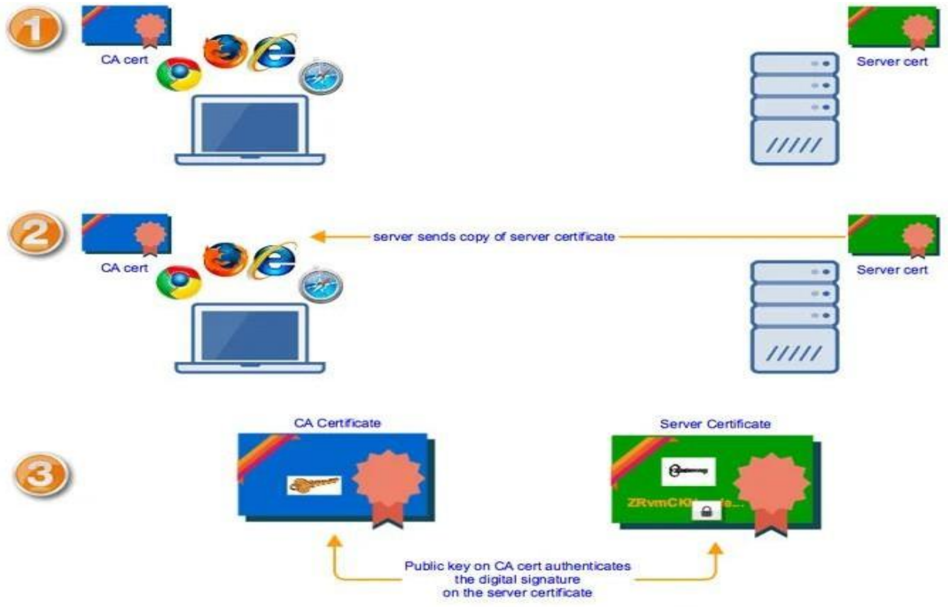


After submitting your CSR and getting your certificate signed, you're well on your way to enhancing your server's security.

Sending of server certificate during SSL Handshake

- Before a browser and an HTTPS server can exchange data over an encrypted connection, they first engage in a process known as the SSL handshake.
- One important part in the SSL handshake is sending the server certificate to the web browser. It's here when the Web browser is able to authenticate the identity of the server it's connecting to.
- When the browser receives a copy of the server certificate, it checks which CA signed the server cert and then retrieves the CA certificate of that particular Certificate Authority. It then uses the CA certificate's public key to verify the server cert's digital signature.

To illustrate,

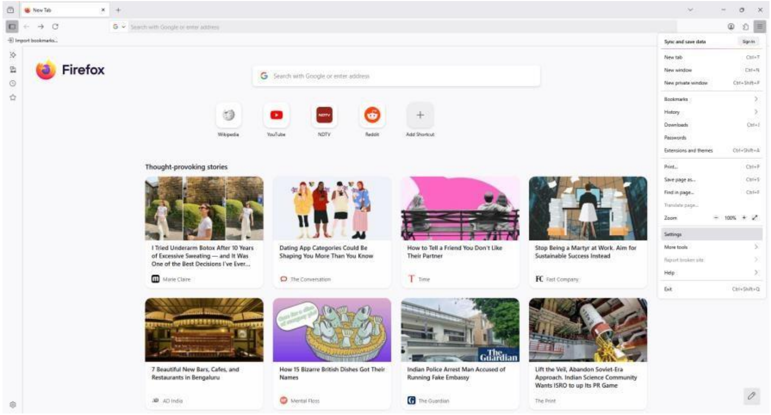


Once the digital signature has been authenticated, the browser and server can proceed with the rest of the SSL process.

STEPS TO CHECK BROWSER CERTIFICATES(Built-in)

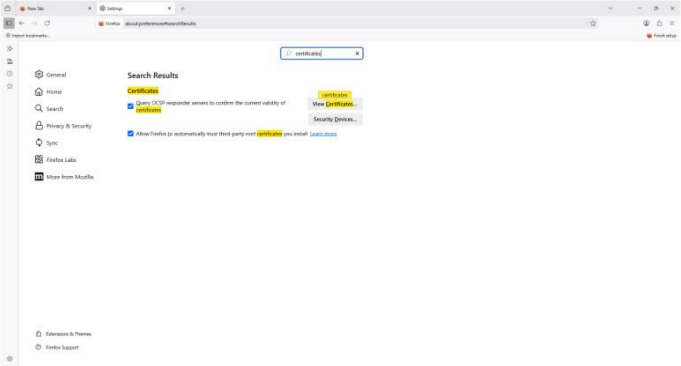
STEP 1:

Open Firefox and click on setting.



STEP 2:

Search for certificates in find in settings. Select view certificates.



about:preferences#searchResults

certificates

Search Results

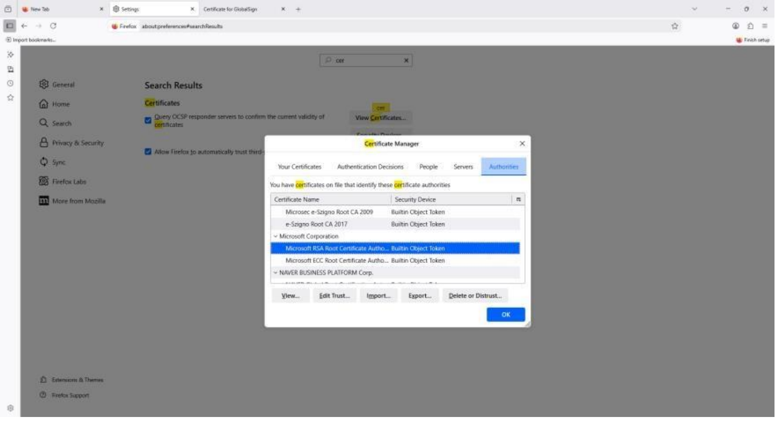
Certificates

☑ Query OCSP responder servers to confirm the current validity of certificates

☑ Allow Firefox to automatically trust third-party root certificates you install

STEP 3:

Now you can view the list of all built-in certificates.

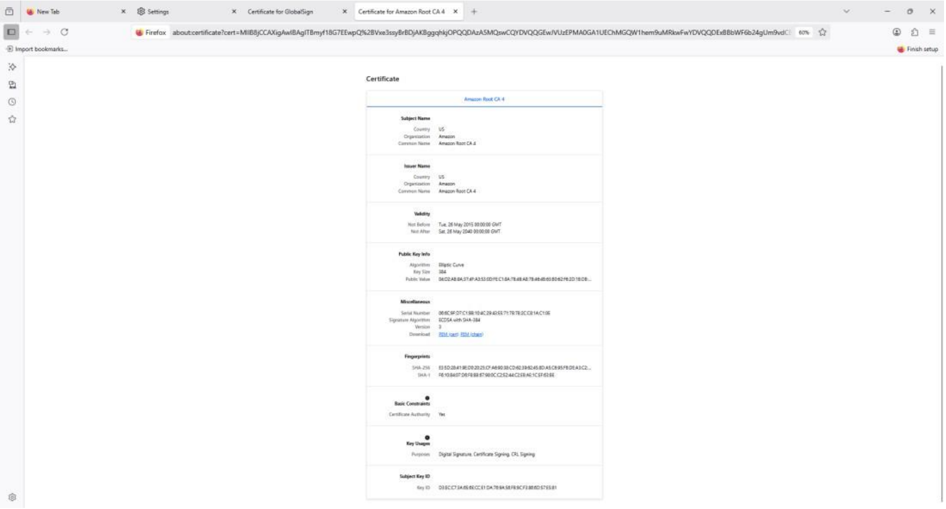


Certificate Manager

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
Microsec e-Szigno Root CA 2009	Builtin Object Token
e-Szigno Root CA 2017	Builtin Object Token
Microsoft Corporation	
Microsoft RSA Root Certificate Autho...	Builtin Object Token
Microsoft ECC Root Certificate Autho...	Builtin Object Token
NAVER BUSINESS PLATFORM Corp.	

You can select and view the certificates. Which contains all the information of the certificates.



Certificate

Amazon Root CA 4

Subject Name

Country US
Organization Amazon
Common Name Amazon Root CA 4

Issuer Name

Country US
Organization Amazon
Common Name Amazon Root CA 4

Validity

Not Before Tue, 26 May 2015 00:00:00 GMT
Not After Sat, 26 May 2040 00:00:00 GMT

Public Key Info

Algorithm Elliptic Curve
Key Size 384
Public Value 04:D2:AB:8A:37:4F:A3:53:0D:FE:C1:8A:7B:4B:A8:7B:46:4B:63:B0:62:F6:2D:1B:DB:...

Miscellaneous

Serial Number 06:6C:9F:D7:C1:BB:10:4C:29:43:E5:71:7B:7B:2C:C8:1A:C1:0E
Signature Algorithm ECDSA with SHA-384
Version 3
Download PEM (cert) PEM (chain)

Fingerprints

SHA-256 E3:5D:28:41:9E:D0:20:25:CF:A6:90:38:CD:62:39:62:45:8D:A5:C6:95:FB:DE:A3:C2:...
SHA-1 F6:10:84:07:D6:F8:BB:67:98:0C:C2:E2:44:C2:EB:AE:1C:EF:63:BE

Basic Constraints

Certificate Authority Yes

Key Usages

Purposes Digital Signature, Certificate Signing, CRL Signing

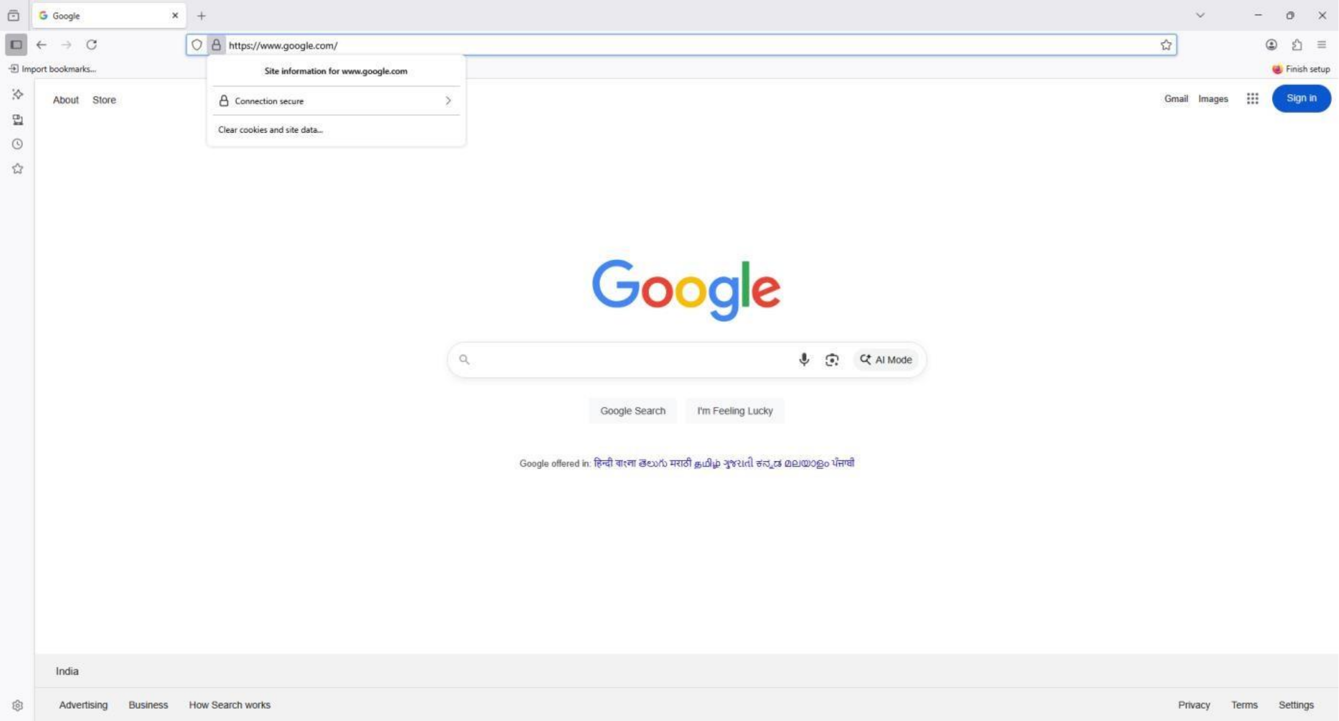
Subject Key ID

Key ID D3:EC:C7:3A:65:6E:CC:E1:DA:76:9A:56:FB:9C:F3:86:6D:57:E5:81

STEPS TO CHECK WEBSITE CERTIFICATES:

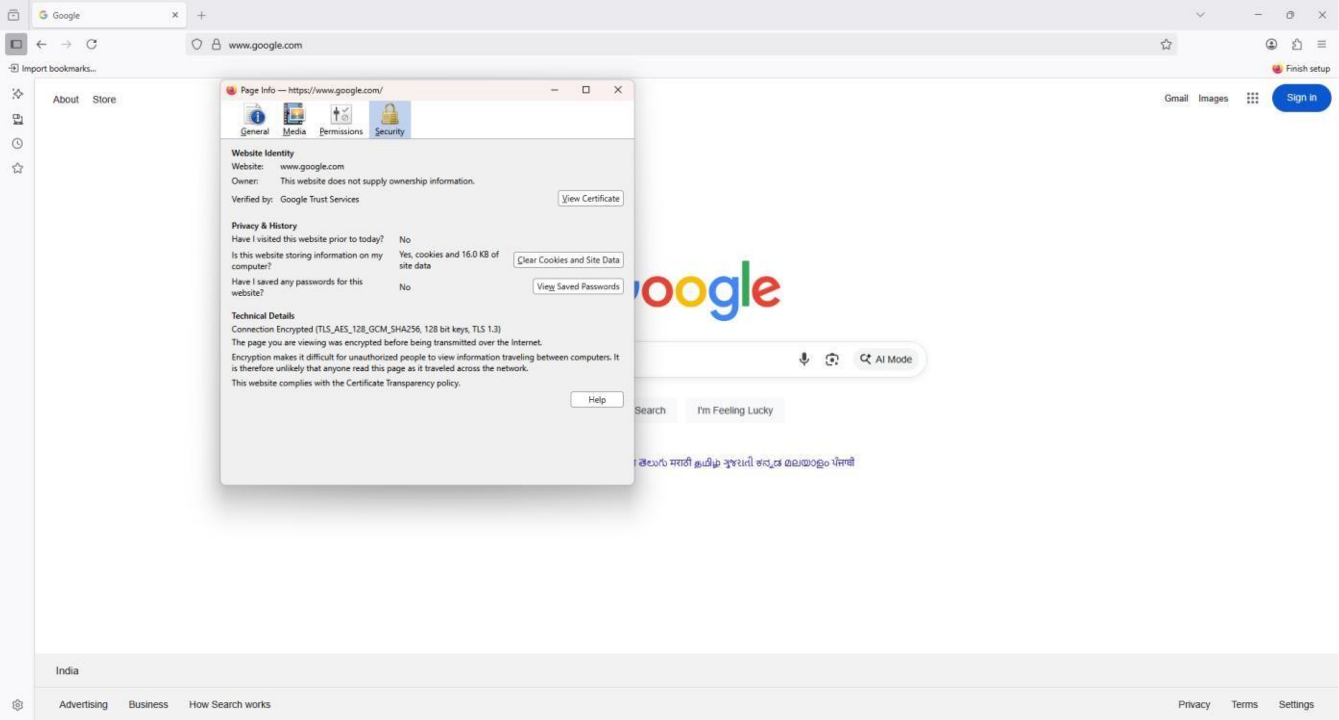
STEP 1:

Open any website. You can recognize the **padlock icon** and `https://` in the browser address bar.



STEP 2:

Click on connection secure > more information >



Page Info — https://www.google.com/

Website Identity

Website: www.google.com

Owner: This website does not supply ownership information.

Verified by: Google Trust Services

Privacy & History

Have I visited this website prior to today? No

Is this website storing information on my computer? Yes, cookies and 16.0 KB of site data

Have I saved any passwords for this website? No

Technical Details

Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)

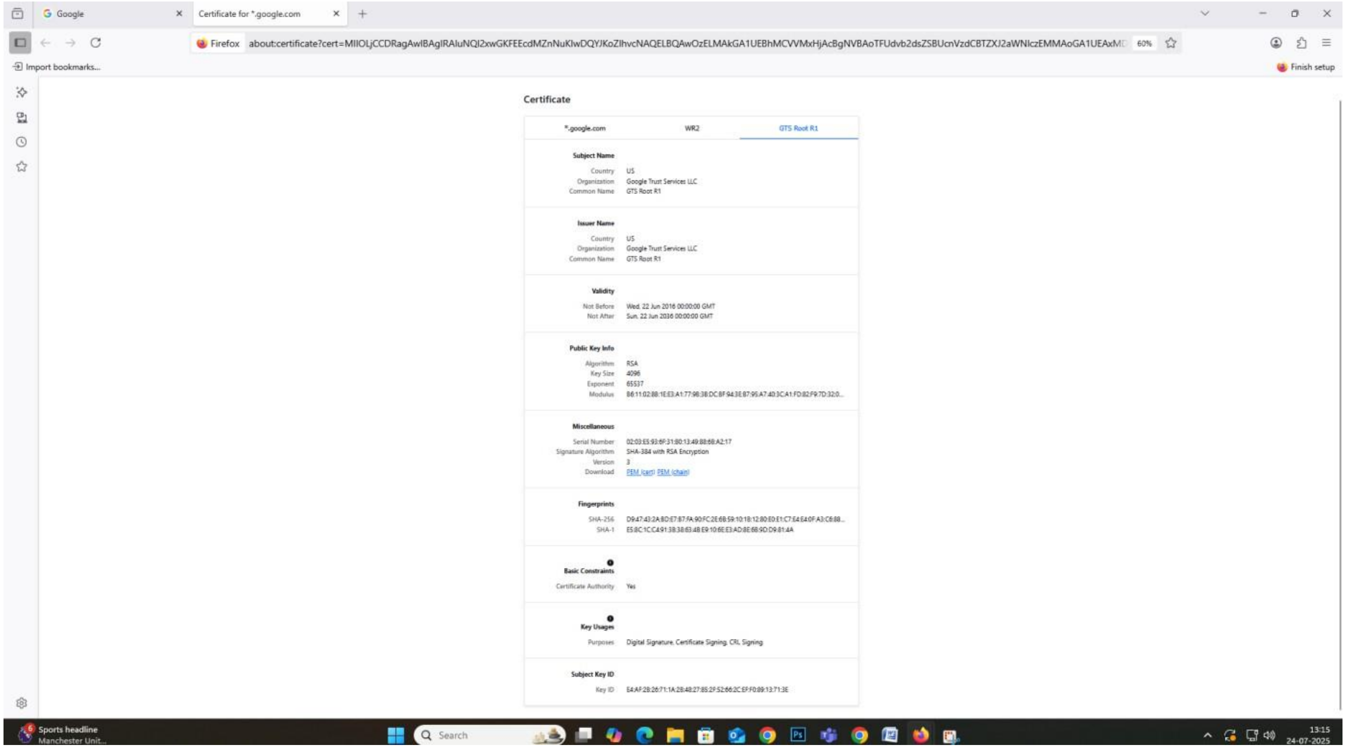
The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

This website complies with the Certificate Transparency policy.

STEP 3:

Click on View certificate


Google
Certificate for *.google.com
Firefox
about:certificate?cert=MIIOLjCCDRagAwIBAgIRAIuNQI2xwGKFEEcdMZnNuKIwDQYJKoZIhvcNAQELBQAwOzELMAkGA1UEBhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBUcnVzdCBTZXJ2aWNlczEMMAoGA1UEAxM
60%
Import bookmarks...
Finish setup
Sports headline
Manchester Unit...
Search
13:15
24-07-2025

Certificate

*.google.com | WR2 | GTS Root R1

Subject Name
Country US
Organization Google Trust Services LLC
Common Name GTS Root R1

Issuer Name
Country US
Organization Google Trust Services LLC
Common Name GTS Root R1

Validity
Not Before Wed, 22 Jun 2016 00:00:00 GMT
Not After Sun, 22 Jun 2036 00:00:00 GMT

Public Key Info
Algorithm RSA
Key Size 4096
Exponent 65537
Modulus B6:11:02:8B:1E:E3:A1:77:9B:3B:DC:BF:94:3E:B7:95:A7:40:3C:A1:FD:82:F9:7D:32:0...

Miscellaneous
Serial Number 02:03:E5:93:6F:31:B0:13:49:88:6B:A2:17
Signature Algorithm SHA-384 with RSA Encryption
Version 3
Download PEM (cert) PEM (chain)

Fingerprints
SHA-256 D9:47:43:2A:BD:E7:B7:FA:90:FC:2E:6B:59:10:1B:12:80:E0:E1:C7:E4:E4:0F:A3:C6:88...
SHA-1 E5:8C:1C:C4:91:3B:38:63:4B:E9:10:6E:E3:AD:8E:6B:9D:D9:81:4A

Basic Constraints
Certificate Authority Yes

Key Usages
Purposes Digital Signature, Certificate Signing, CRL Signing

Subject Key ID
Key ID E4:AF:2B:26:71:1A:2B:48:27:85:2F:52:66:2C:EF:F0:89:13:71:3E

Now you can see all the details of the certificates