Secure Sockets

Part 3 – Certificates

Barak Gonen

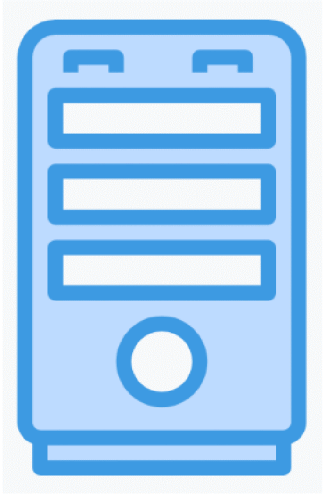
Part 3 – Certificates

- Certificate Authority
- Certificate Chain
- Certificate Types
- Certificate Revocation
  - OCSP

Authentication by Certificates

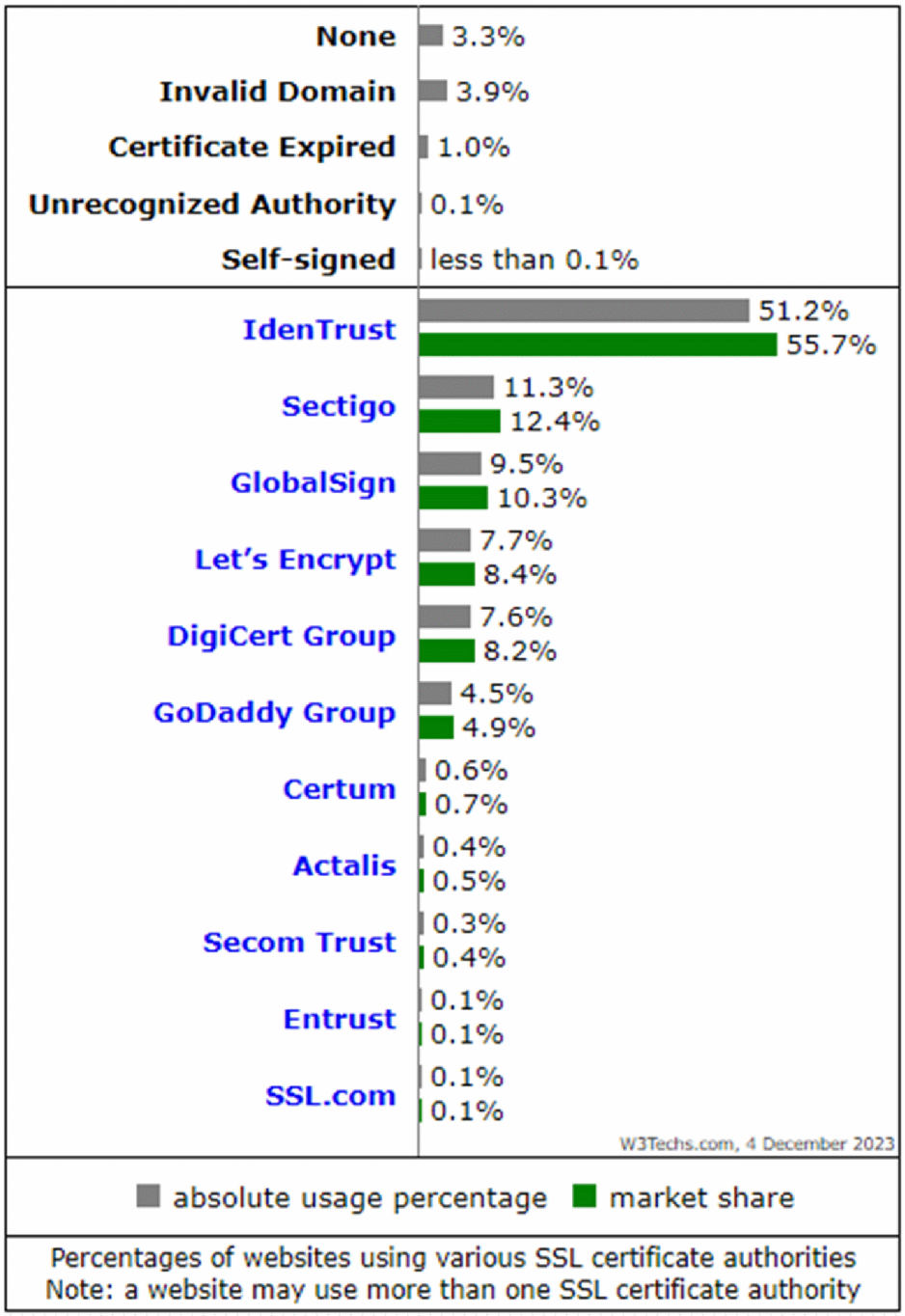
Public Key Infrastructure

- Client
- Server
- **Certificate Authority**



Certificate Authority – CA

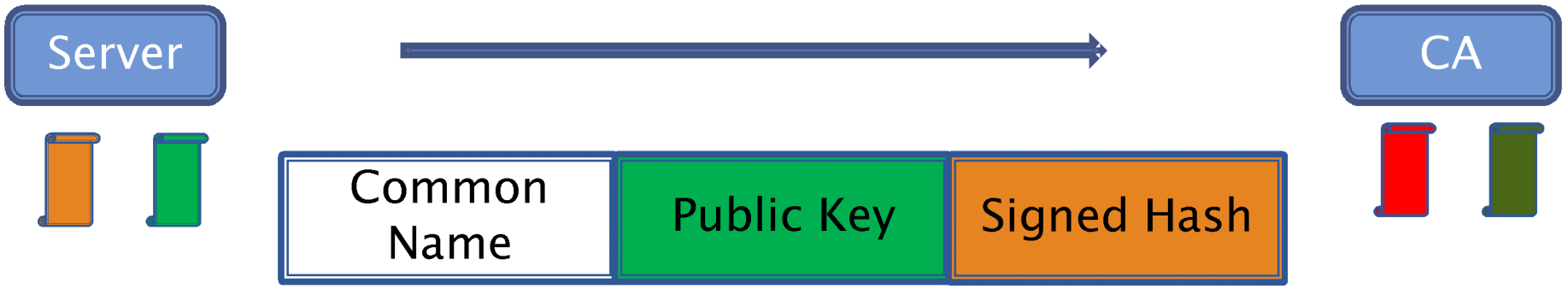
- Anchor of trust between clients and servers
- Five companies manage majority of Internet certificates
- Their public keys are in the browsers' code
  - Certmgr.msc
- Look for Root CA's in your PC's table
  - "Friendly name" field
  - Who signs the root CAs certificates?



https://w3techs.com/technologies/overview/ssl_certificate

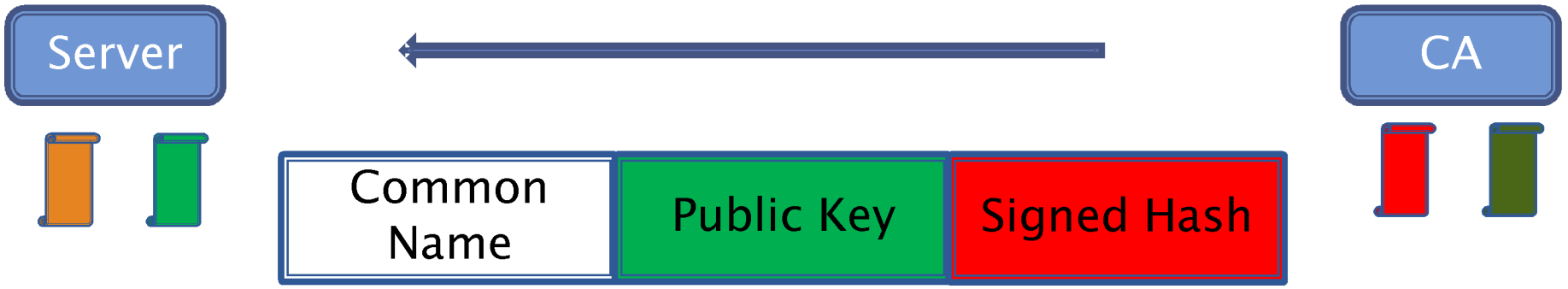
Certificate Signing Request

- Server sends a CSR to the CA:
  - Server's domain name ("common name")
  - The public key of the domain
  - Hash of the CSR, signed with the domain's private key



Certificate

- The CA responds with a certificate:
  - Server's domain name
  - Server's public key
  - Digital signature- hash with the CA's private key
- Browsers have the CA public key pre-installed, so the digital signature can be verified

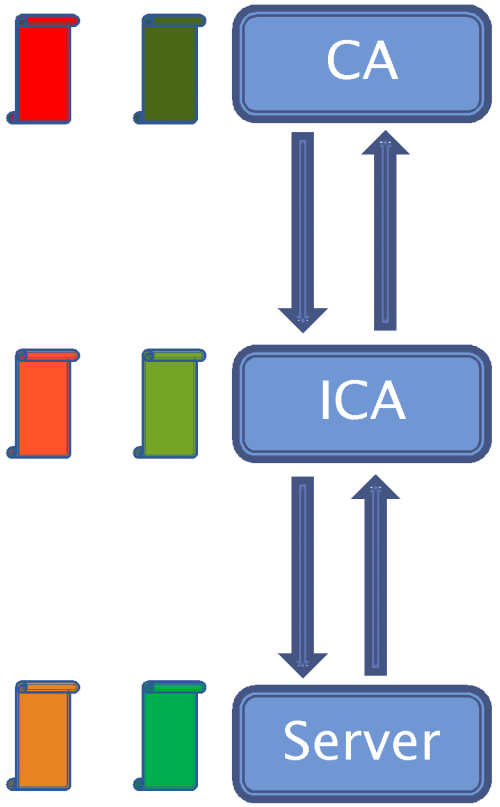


Certificate Types

- DV- Domain Validation
  - Approves the domain name belongs to the certificate holder
- OV – Organization Validation
  - Approves the certificate holder is a real institute. Tax records, company records
- EV – Extended Validation
  - Approves the certificate holder has physical offices, company history
  - Not an attempt of an internal employee to conduct fraud

Certificate Chain

- If the CA's private key is detected, a browser software update is required.
- We would like the CA to sign as little as possible.
- We will create an "intermediary" – Intermediate CA.
  - The ICA will receive a signature from the Root CA,
  - The ICA will sign the Certificates itself,
- If the ICA key is discovered, it will be replaced and receive a new certificate.



Certificate Chain– cont.

- Problem – anyone with a certificate, can start signing certificates
- Solution:
  - Authorization as signing authority is part of the certificate
  - If a signing authority is credited, decreasing level counter is included

Server	Signing Authority	Level Counter
Root CA	Yes	1
ICA	Yes	0
Example.com	No	–

Certificate Authority Authorization

- How can we prevent an imposter from getting a real certificate from an ICA to our domain?
- Solution – CAA record in the DNS
  - Linux (or WSL on Windows): `dig domain caa`

Viewing a Certificate

- WSL
  - openssl s_client -connect example.com:443 | openssl x509 -text -noout
- Browser
- RSA reminder:
  - Cipher = (Plain^E) mod N
  - Plain = (Cipher^D) mod N
  - The other side is given:
    - N (“Modulus)
    - E (“Exponent”)
    - To find the private key, N must be decomposed to PxQ

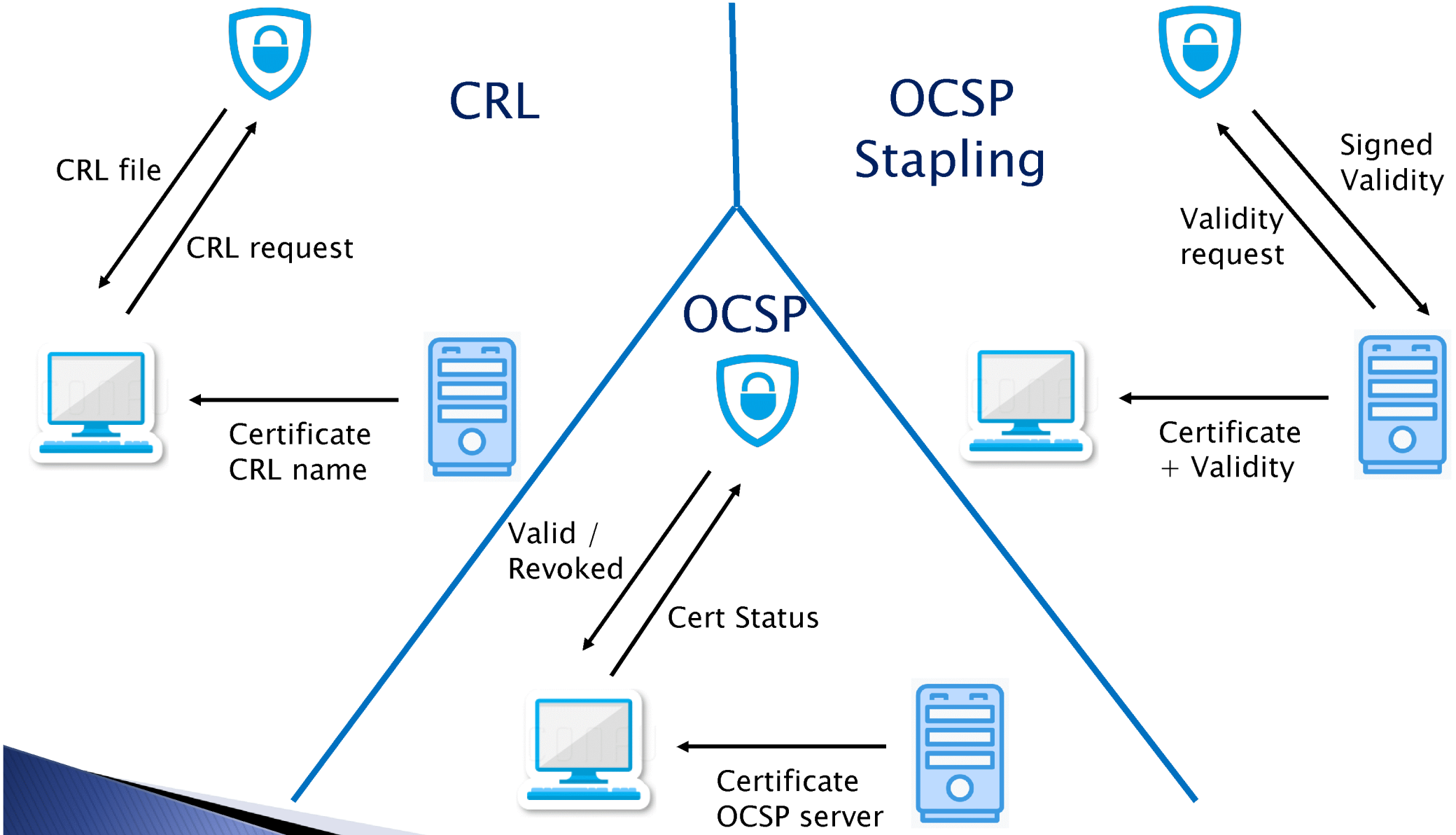
P = 17
Q = 23
N = 391 (PxQ)
T = 352 (P-1)(Q-1)
E = 113 (Public)
D = 81 (Private)

```
guys@LAPTOP-SFOC9S2J:~$ openssl s_client -connect jct.ac.il:443 | openssl x509 -text -noout
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = R3
verify return:1
depth=0 CN = jct.ac.il
verify return:1
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:d1:d7:a8:29:d4:6a:f8:8d:01:64:ee:08:81:54:ec:c6:63
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = Let's Encrypt, CN = R3
        Validity
            Not Before: Oct  9 16:37:17 2023 GMT
            Not After : Jan  7 16:37:16 2024 GMT
        Subject: CN = jct.ac.il
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a2:40:04:d5:d4:bb:e6:96:95:ba:ae:e8:9d:96:
                    b5:10:1e:2b:d3:9a:f1:46:d1:37:c2:de:5d:a1:cd:
                    9c:d4:1d:ba:e1:04:18:de:93:36:5b:ef:27:7d:90:
                    26:98:0f:63:e5:f3:ad:dc:9b:77:b6:4a:05:04:77:
                    a9:6a:09:6e:7e:5b:b5:2b:95:7c:94:1f:a6:5d:55:
                    8f:a3:d6:35:b0:3d:fd:65:be:b3:a5:b8:48:17:47:
                    18:d3:55:01:e6:31:10:ae:91:88:60:87:4d:2b:d8:
                    ee:be:75:74:b4:37:b8:71:75:b5:52:92:31:48:d3:
                    61:7a:ca:77:26:34:e4:c8:2b:38:84:97:e0:37:cb:
                    1a:32:10:f8:30:99:56:f2:99:a3:9f:66:ed:d3:7a:
                    0c:8d:ea:82:6e:6f:79:39:2b:34:86:88:4f:14:ab:
                    17:84:32:2b:79:db:88:84:8b:5f:3a:f6:c9:3a:ef:
                    12:cd:35:9f:59:88:15:6e:37:ad:d3:0e:e8:a5:20:
                    d6:f4:5f:f0:3f:93:07:06:10:e1:16:6b:b3:c5:fb:
                    56:7f:5c:14:03:24:a6:15:be:d7:1f:4d:f7:57:e8:
                    7b:9f:c9:7e:39:34:21:26:41:7b:f5:67:f8:6b:d0:
                    7b:0e:e6:1e:b8:97:0a:95:3f:92:a1:19:5d:69:28:
                    0e:2b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
```

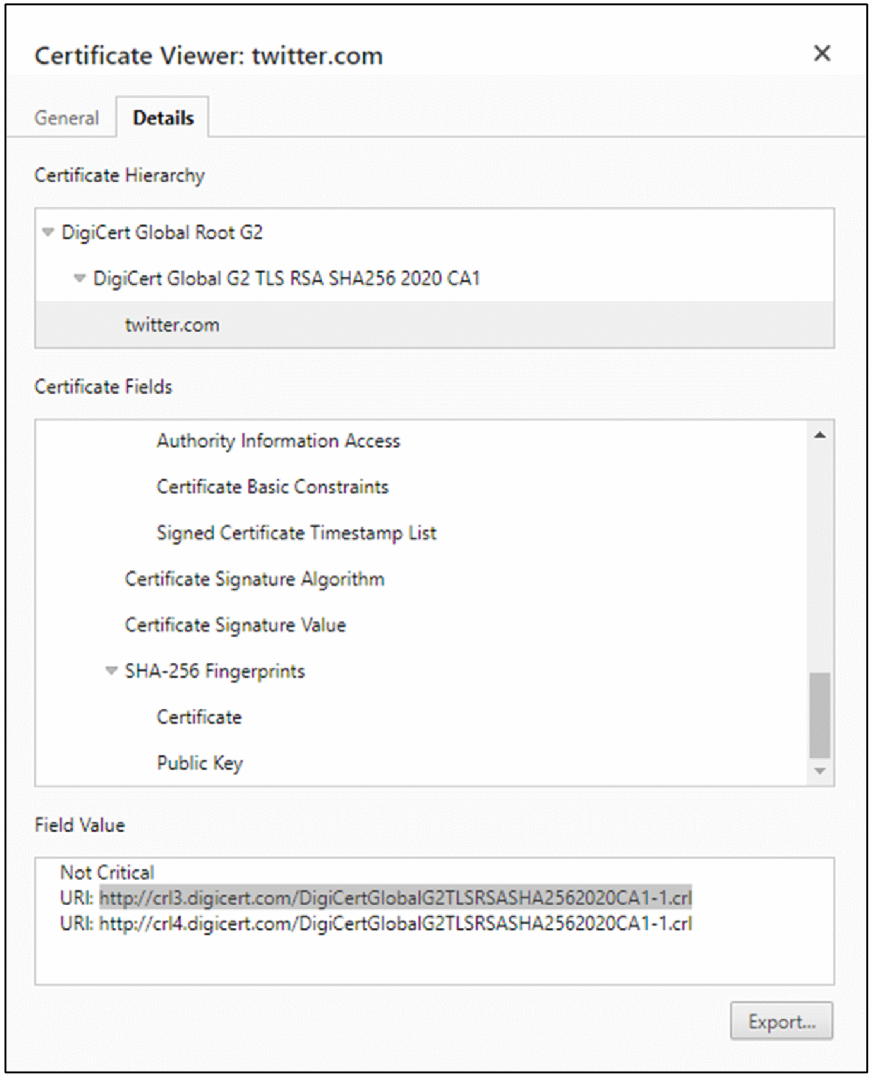
Certificate Revocation Status

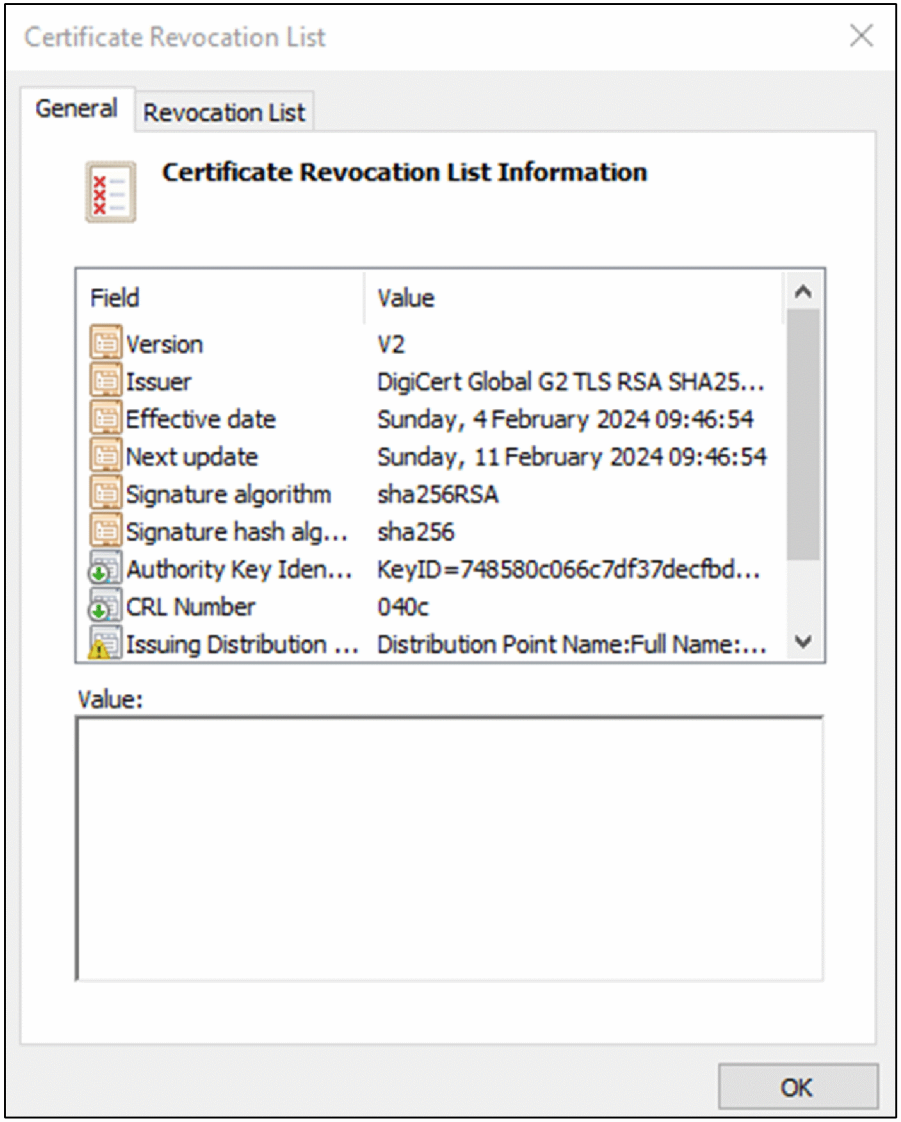
- Certificates might need to be revoked
  - Private key compromised or domain closed
- How can one tell if a certificate is valid?
  - CRL – Certificate Revocation List
  - OCSP – Online Certificate Status Protocol
  - OCSP Stapling

Certificate Revocation Status



CRL


Certificate Viewer: twitter.com
General
Details
Certificate Hierarchy
DigiCert Global Root G2
DigiCert Global G2 TLS RSA SHA256 2020 CA1
twitter.com
Certificate Fields
Authority Information Access
Certificate Basic Constraints
Signed Certificate Timestamp List
Certificate Signature Algorithm
Certificate Signature Value
SHA-256 Fingerprints
Certificate
Public Key
Field Value
Not Critical
URI: http://crl3.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-1.crl
URI: http://crl4.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-1.crl
Export...


Certificate Revocation List
General
Revocation List
Certificate Revocation List Information
Field
Value
Version
V2
Issuer
DigiCert Global G2 TLS RSA SHA25...
Effective date
Sunday, 4 February 2024 09:46:54
Next update
Sunday, 11 February 2024 09:46:54
Signature algorithm
sha256RSA
Signature hash alg...
sha256
Authority Key Iden...
KeyID=748580c066c7df37decfbd...
CRL Number
040c
Issuing Distribution ...
Distribution Point Name:Full Name:...
Value:
OK

OCSP Stapling