Secure Sockets

Part 3 – Certificates

Barak Gonen

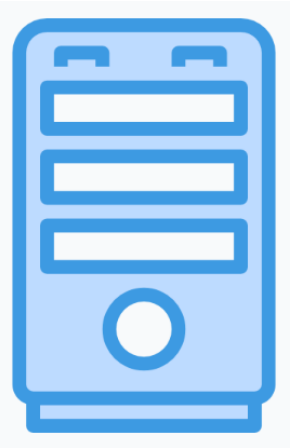
Part 3 – Certificates

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

Authentication by Certificates

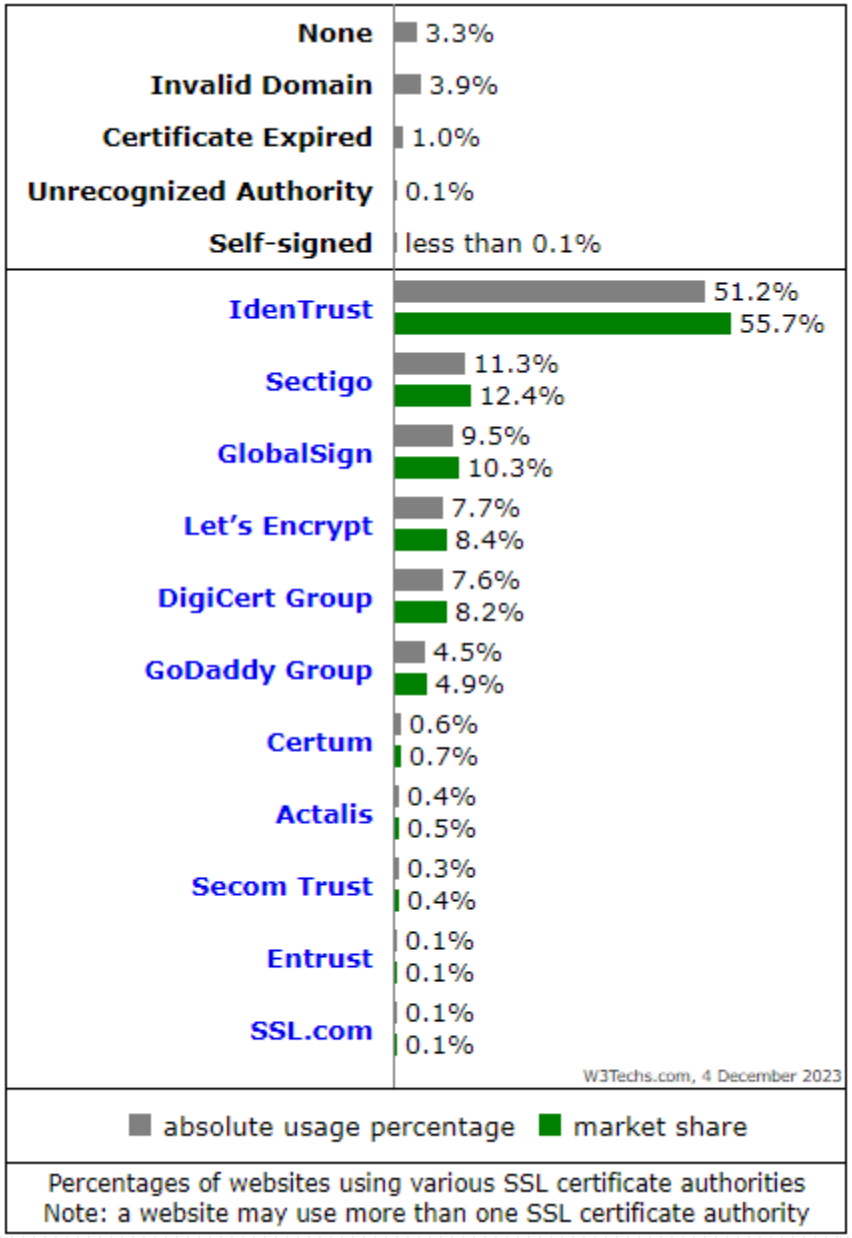
Public Key Infrastructure

- Client
- Server
- **Certificate Authority**



Certificate Authority – CA

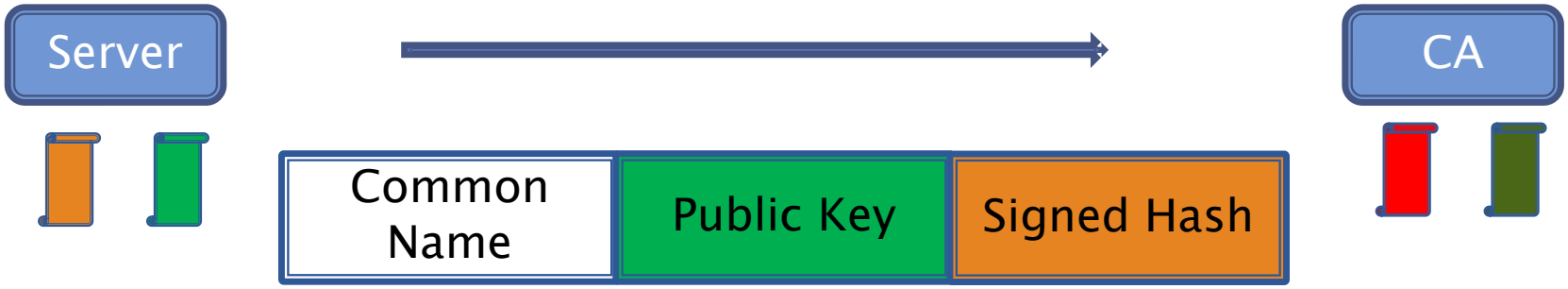
- Anchor of trust between clients and servers
- Five companies manage majority of Internet certificates
- Their public keys are in the browsers' code
  - Certmgr.msc
- Look for Root CA's in your PC's table
  - "Friendly name" field
  - Who signs the root CAs certificates?



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

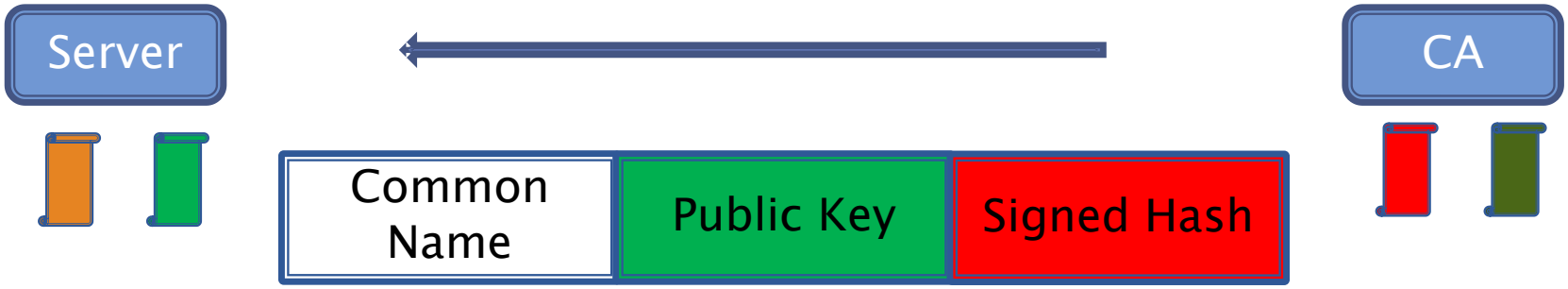
Certificate Signing Request

- 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

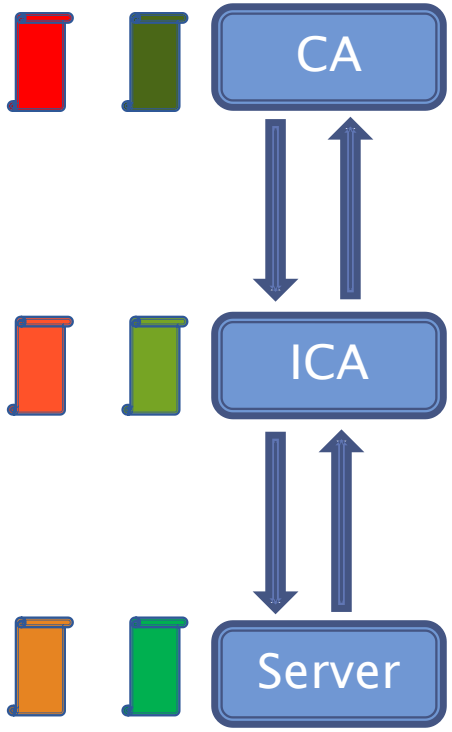


Certificate Types

- 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)

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