Hansel & Gretel do TLS

by

Marcus Bointon

Synchromedia Limited

Smartmessages.net

Radically Open Security

What is TLS?

- Transport Layer Security protocol
- The new(ish) name for SSL - Since 1999
  - Versions: SSLv2, SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3
- A set of standards for security & encryption
- Can wrap around any higher-level protocol
  - HTTP, SMTP, FTP, IMAP, DNS, etc
- Popular implementations: OpenSSL, LibreSSL, BoringSSL

Why use TLS?

- Provides confidentiality, authenticity & integrity
- Better performance with HTTP/2
- Google will rank you higher
- Required for iOS apps
- Chrome 50 disabled HTTP GeoLocation
- Keeps the wicked witch out

Toolkit: Hashes, MACs, Ciphers & KX

- Hashes produce a fixed-length digest from data; integrity
  - ~~MD5~~, ~~SHA1~~, SHA2 (SHA256, SHA384, SHA512)
- Message Authentication Code (MAC): data + a key; authenticity
  - ~~HMAC-MD5~~, HMAC-SHA256, Poly1305
- Ciphers; encryption algorithms; confidentiality
  - Integer factoring, elliptic curve ("EC"), symmetric, asymmetric
  - ~~RC4~~, AES, ~~3DES~~, RSA, ChaCha20
- Key Exchange
  - ~~RSA~~, Diffie-Hellman ("DH"), x25519, x448, EC, "Ephemeral", ECDHE

New in TLS 1.3

- Removal of all weak and legacy algorithms & extensions
- Moar encryption
- Lower handshake overhead
- All ciphers support forward secrecy
- Elliptic curve ciphers as standard
- Downgrade protection

TLS 1.3 Handshake

ClientHello
Cipher Suite List
Key Share

ServerHello
Cipher Suite
Key Share
Certificate & Signature
Server **Finished**

Client **Finished**
HTTP Request

HTTP Response

200ms

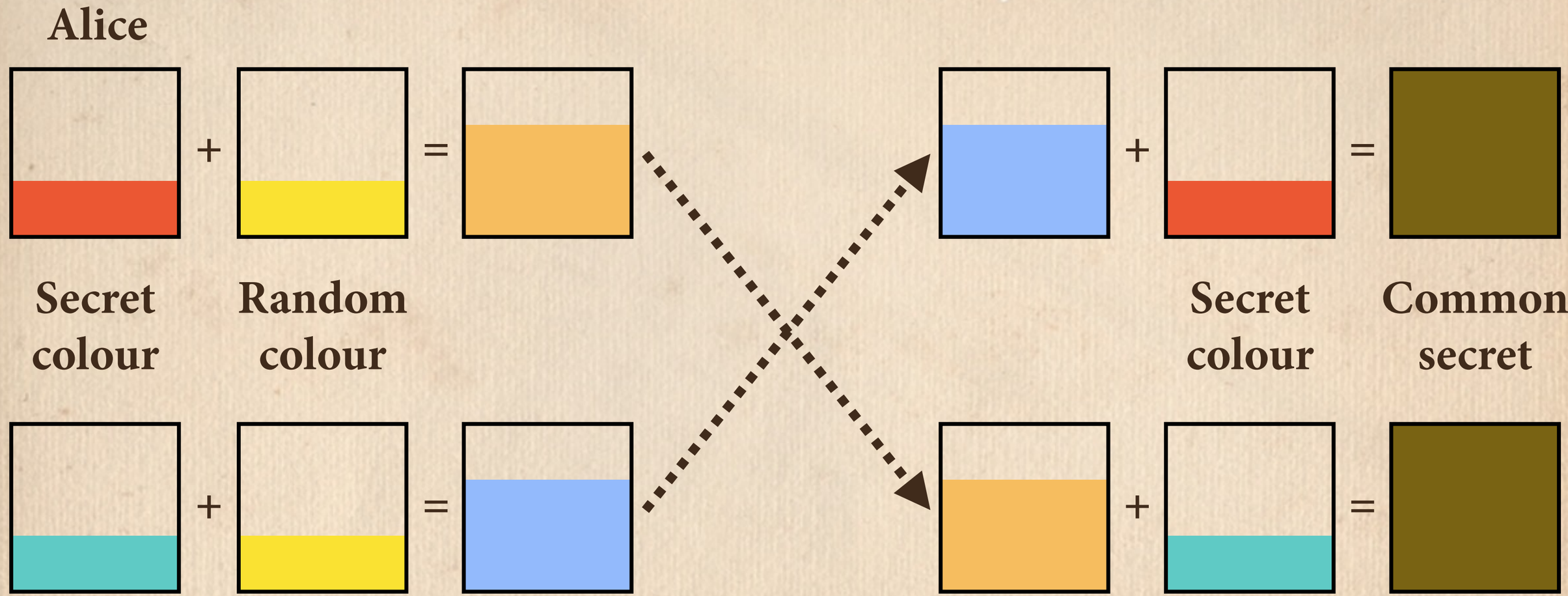
TLS 1.3 *Resumption*

`ClientHello`
Session ticket
Key Share
HTTP **`GET`**

`ServerHello`
Key Share
Server **`Finished`**
HTTP Response

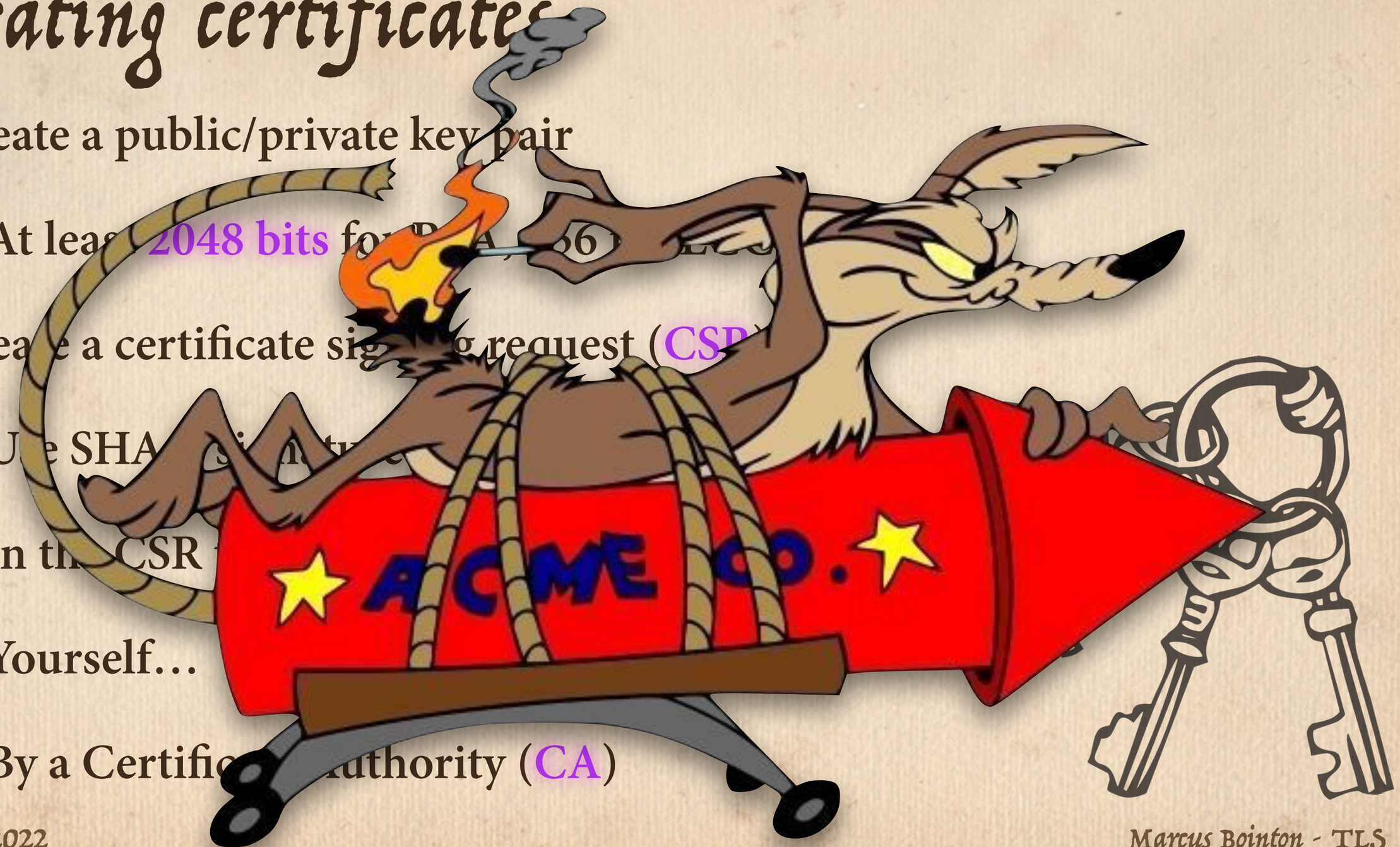
0-RTT!

Diffie-Hellman Key Exchange



Creating certificates

- Create a public/private key pair
  - At least 2048 bits for RSA, 256 bits for ECC
- Create a certificate signing request (CSR)
  - Use SHA-256 signature
- Sign the CSR
  - Yourself…
  - By a Certificate Authority (CA)



Certificate chains

Root CA certificate

Root CA certificate

Intermediate CA certificate

Site certificate

Browser & OS

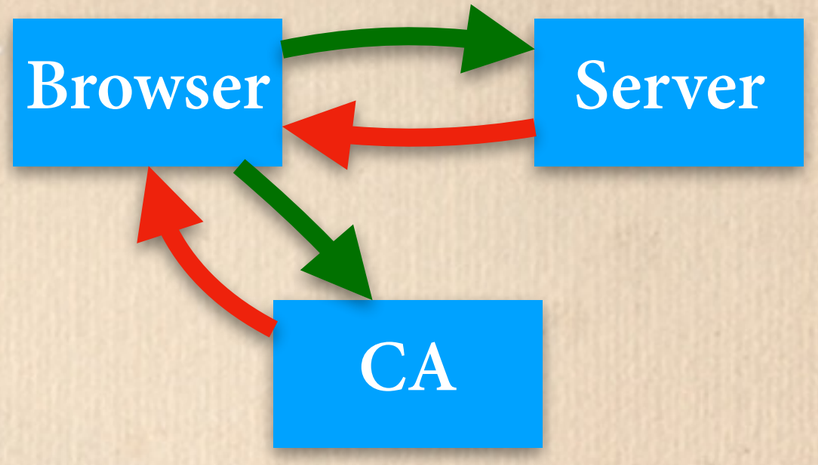
certificate store

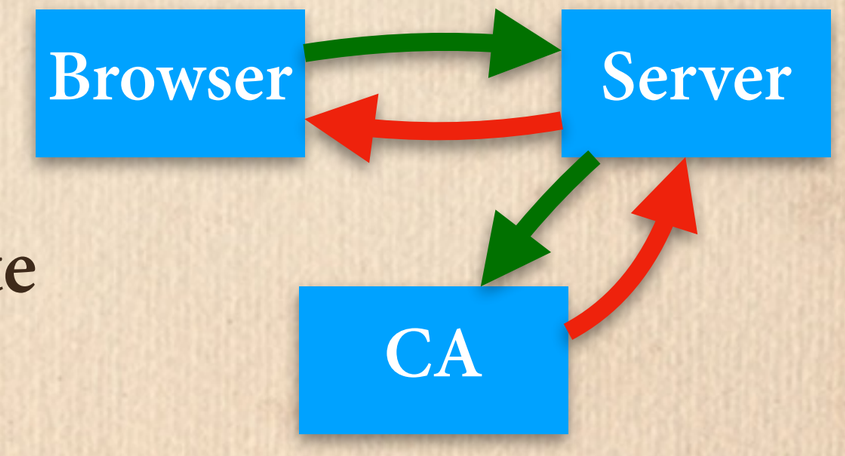
Server

certificate store

CRLs, OCSP & Stapling

- How to find out if a cert has been revoked?
- Browser asks the CA — OCSP
  - Our site becomes dependent on CA's site
  - CA's site becomes a privacy leak risk
- Get the server to ask the CA in advance
  - Staple the proof of validity to the certificate
  - Can't fake it because it's signed by the CA



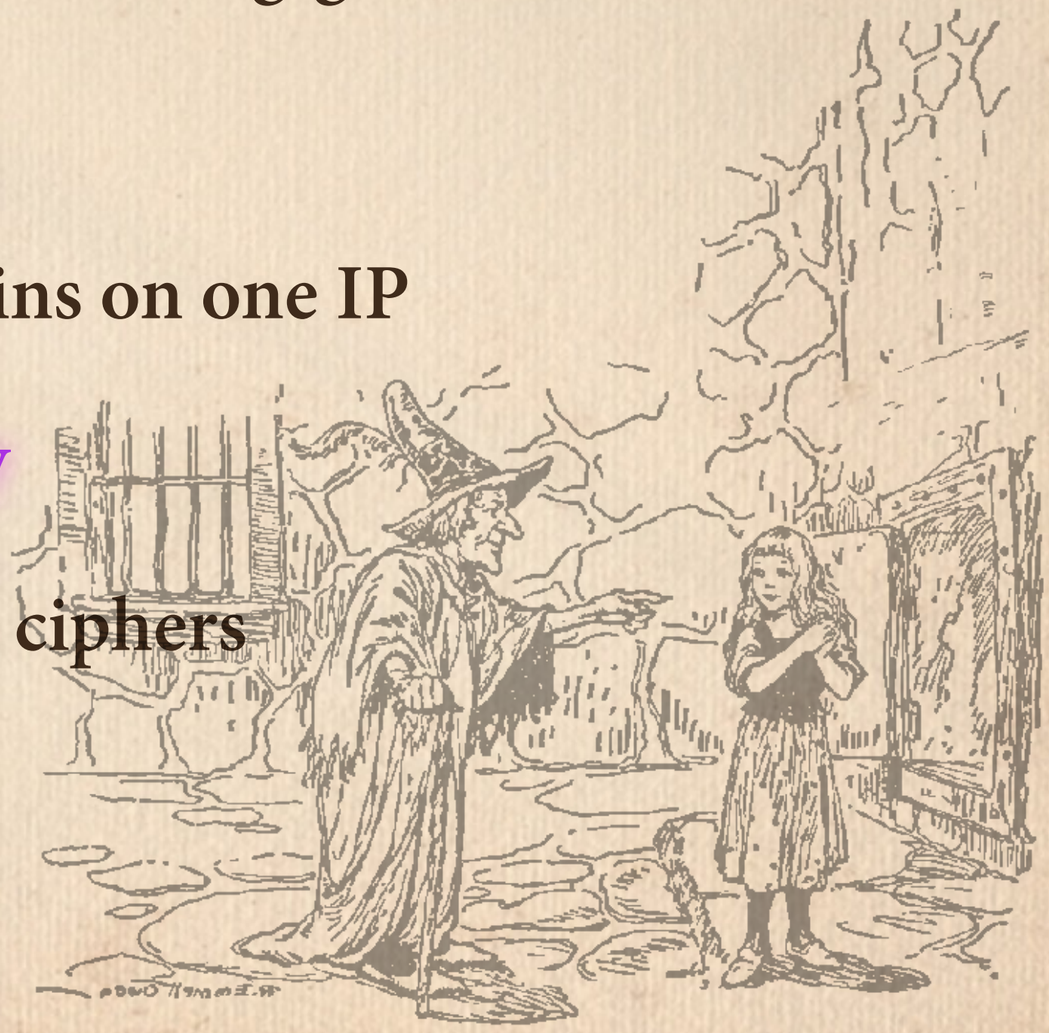


Deploying TLS - App concerns

- Use TLS by default, keeps things simple
- Don't use protocol-relative URLs (//...)
- Avoid mixed mode: https + http
  - HSTS & CSP can auto-upgrade
  - Create proxies if HTTPS not available
- Cookies: set httponly, secure, samesite flags

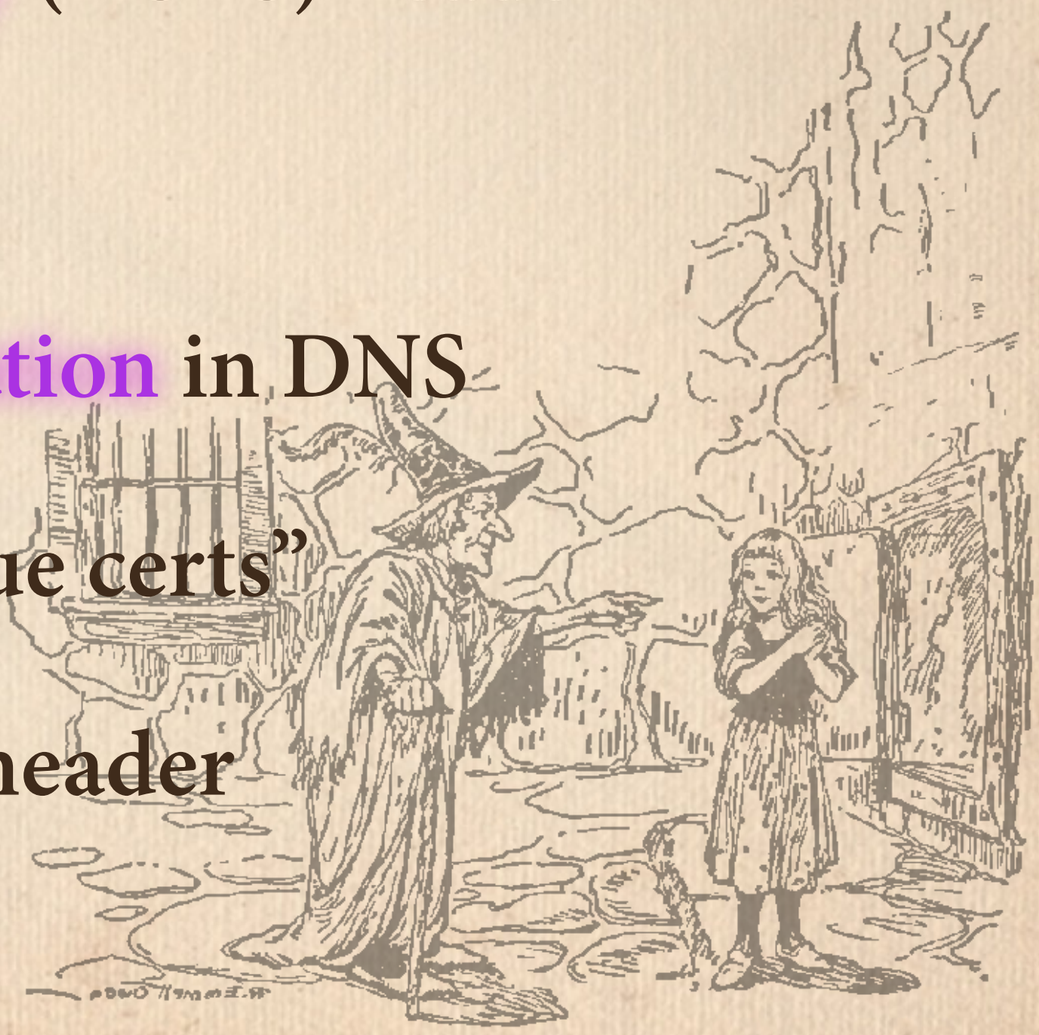
Deploying TLS - Server config

- https://mozilla.github.io/server-side-tls/ssl-config-generator/
- Redirect to secure site
- Use SNI + SAN to host multiple domains on one IP
- Create DH params for forward secrecy
- At least TLSv1.2 — disable old & weak ciphers
- Enable TLS session caching
- Staple CA certs for OCSP



Deploying TLS - Improving security

- HTTP Strict Transport Security (HSTS) header
  - "We always encrypt"
- Certificate Authority Authorisation in DNS
  - "Permit only these CAs to issue certs"
- Content Security Policy (CSP) header
  - "Permit only these sources"



Testing T

Click the pad

securityheaders.io

Security

A+

IP Address:

Report Time:

Headers:

✔ X-Content-Type-Options ✔ X-XSS-Protection

✔ X-Frame-Options ✔ Content-Security-Policy

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > www.smartmessages.net > 2a00:1098:0:80:1000:3b:1:1

SSL Report: www.smartmessages.net (2a00:1098:0:80:1000:3b:1:1)

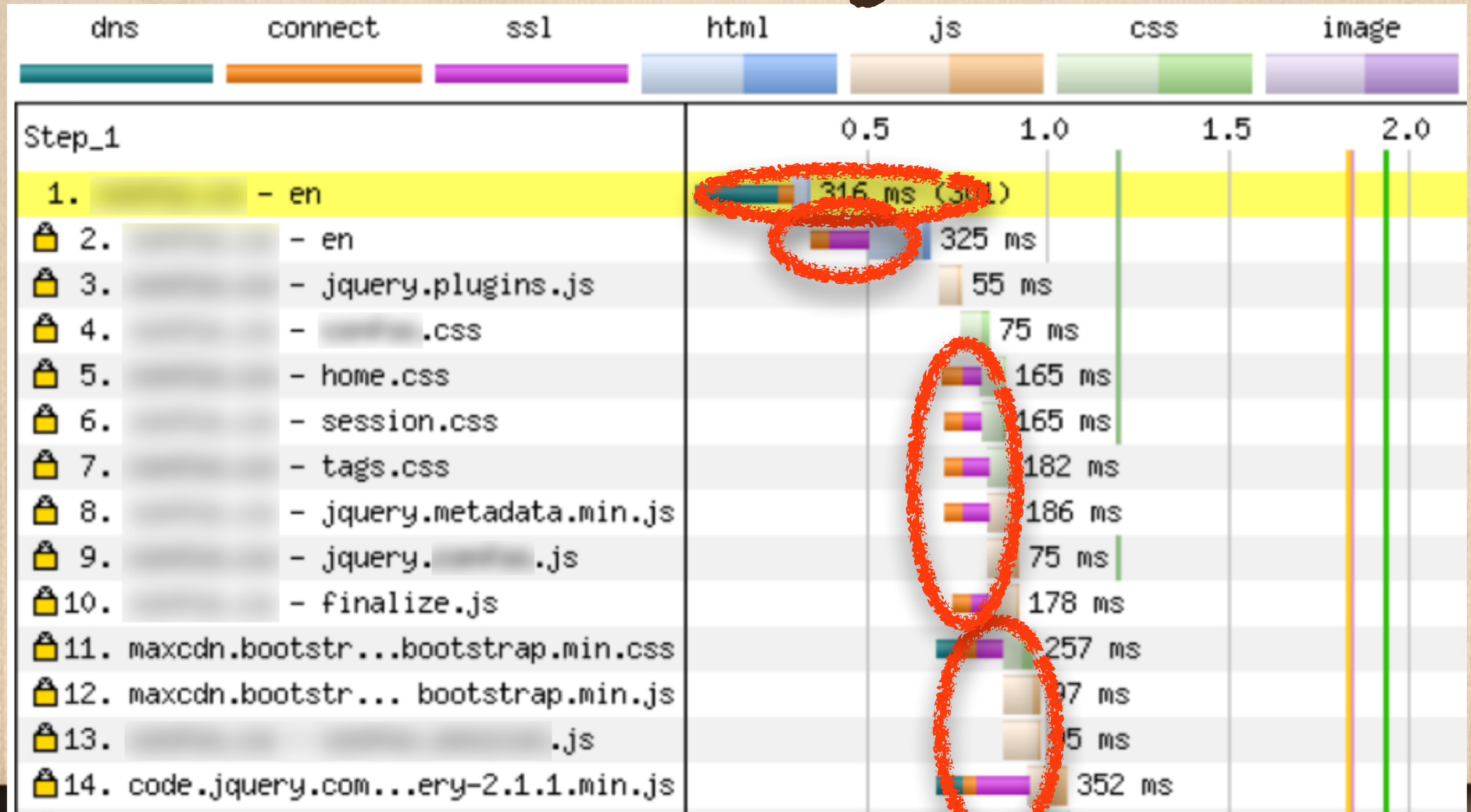
HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

DNS Certification Authority Authorization (CAA) Policy found for this domain. MORE INFO »

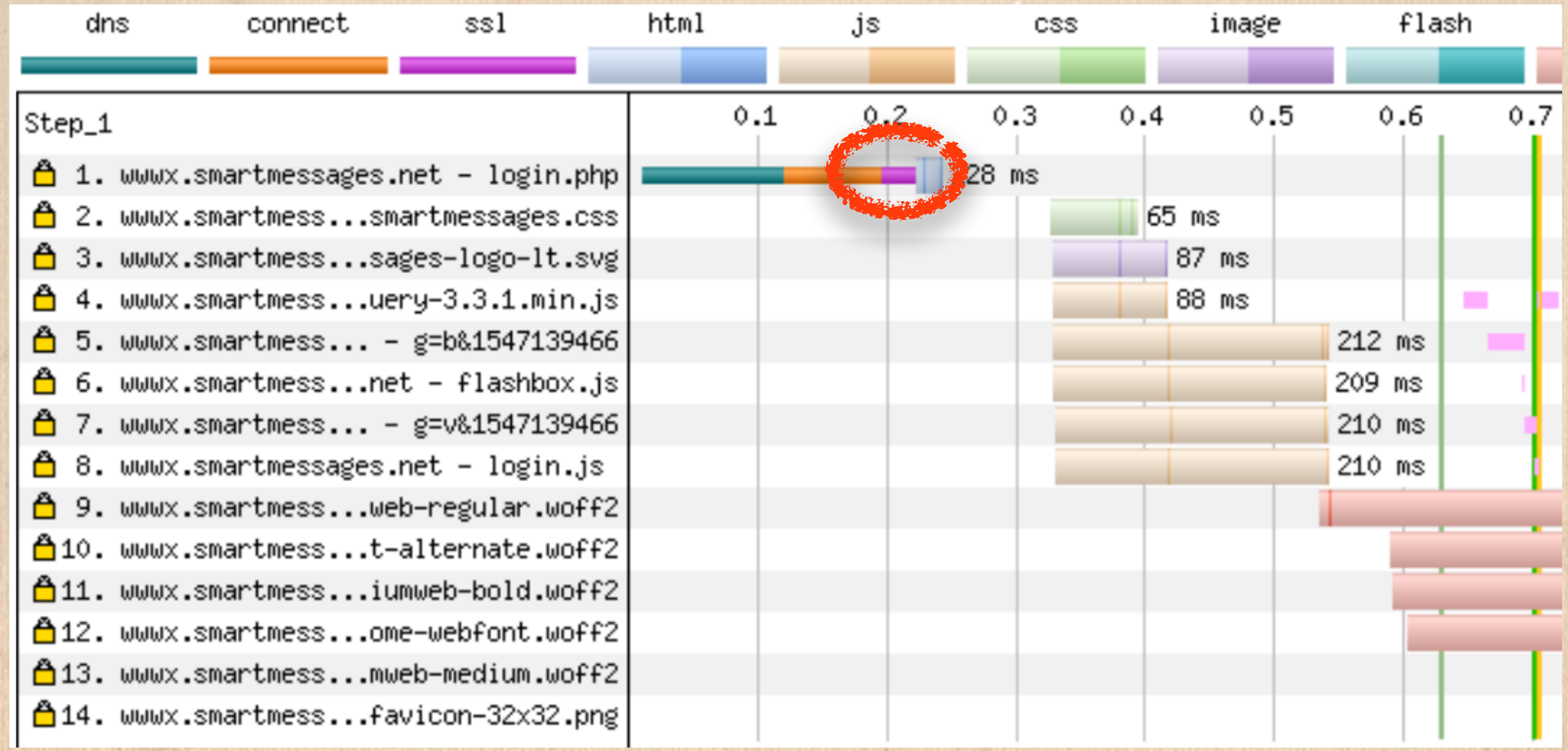
Results for **www.smartmessages.net**

HTTPS by default:	✔ Yes
Content Security Policy:	✔ Good policy
Referrer Policy:	Referrers partially leaked
Cookies:	0
Third-party requests:	0

TLS overhead - old way

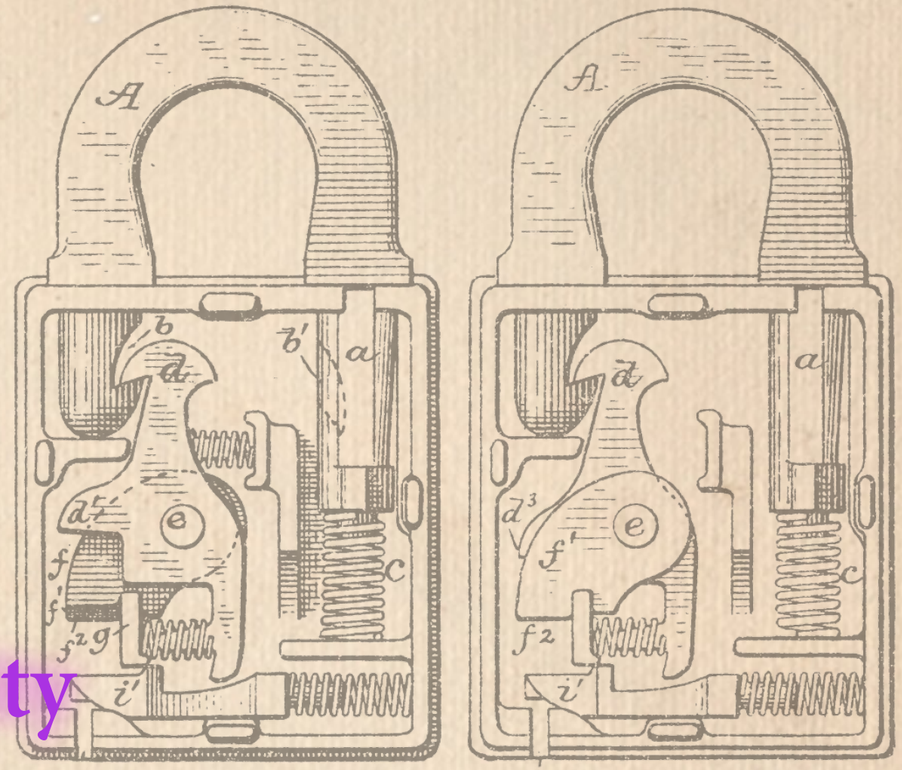


TLS overhead - new way



TLS Summary

- It can be free
- It's fast(er) – use HTTP/2
- Use TLS everywhere by default
- Simple measures maximise security
- Help Hansel & Gretel make it to your site safely



...and they all lived happily ever after

The End

Thank you

ConFoo.ca 20

- Marcus Bointon, marcus@synchromedia.co.uk
- @SynchroM & @PrivacySpider
- Synchro on GitHub & Stack Exchange