IETF 83

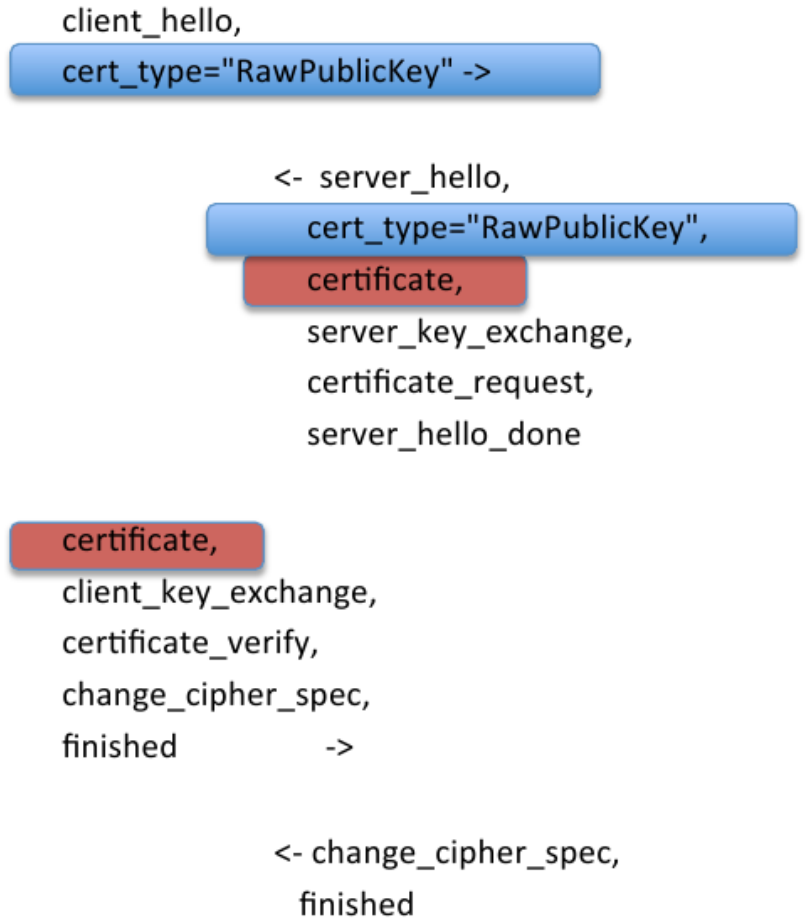
Websec

- HSTS key pinning – draft-ietf-websec-key-pinning-01
  - podobny princip jako HSTS pin
  - hash je z SubjectPublicKeyInfo z certifikatu
    - Chrome to ma presne rovnako

```
Public-Key-Pins: max-age=31536000;
    pin-sha1="4n972HfV354KP560yw4uqe/baXc=";
    pin-sha256="LPJNul+wow4m6DsqxbninhsWHlwfp0JecwQzYpOLmCQ="
```

TLS out-of-band pubkey validation

- miesto certifikatov sa v TLS handshake vymenia kluce
- klient/server musi validovat „out-of band“ ci patria spravnemu vlastnikovi
  - DANE, preconfigured



TLS cached object

- CachedObject object is sent in ClientHello
- ServerHello returns CachedObject
- Instead of sending the Certificate payload with the certs in it only the fingerprint is sent.
- Same for list of Trusted Cas
- Cached Object contains:
  - Type: certificate_chain(1), trusted_cas(2)
  - Hash Algorithm
  - Hash Value
- zmensenie objemu dat v TLS handshake pre pomale kanaly alebo embedded zariadenia

TLS multiple stapled OCSP

- v zasade jako klasicky OCSP stapling
- ale da sa tam narvat OCSP response pre kazdy certifikat z chainu
- vyriesi
  - captive portaly blokujuce OCSP
  - privacy leak (ked sa klient pyta OCSP responderov)

TLS-PWD (dragonfly)

- PAKE (password-based key exchange)
- nesmie byt mozne bruteforcovat offline
- rozdiel proti TLS-SRP
  - moznost menit cyklicku grupu
  - ma ECC
- prelomenie je ekvivalentne prelomeniu Diffie-Hellmana
- zatial popisany len nejaky sileny a neprakticky utok na offline bruteforce, kde sa vyzaduju kompromitovane obe strany
  - je to problem len pri formalnej verifikacii (v random oracle modeli)

Podrobnosti (drafty atd.)

https://tools.ietf.org/agenda/83/