TLS Cached Certificates Extension

Stefan Santesson

AAA-sec.com

Basic idea

- Don’t send known server certificates
- Save bandwidth
  - Latency and error prone connections
  - EAP TLS
- Simple
  - Chop down draft-shacham-tls-fast-track

Proposal

- New hello extension
  - Client: h_1, h_2, … , h_n (Possible known Certs)
  - Server: h_x (Selected Cert) or absent extension
- h_n = Hashed certificate_list element of a server side Certificate message
- On match/accept
  - Server sends h_x as certificate_list in serverside certificate message
  - Rest of handshake proceeds as normal

Syntax

```
struct {
     opaque certificate_hash; <1..2^8-1>
} CachedCerts;

OR

struct {
     HashAlgorithm hash;
     opaque certificate_hash; <1..2^8-1>
} CachedCerts;
```

Questions – Way Forward

- Does problem need to be solved?
- Is this the right approach?

- Hash agility?
- TLS WG item?

Stefan Santesson
stefan@AAA-sec.com