Approaches to HTTPs-based Request Routing and Delegation for Interconnected CDNs

draft-slovetskiy-cdni-https-delegation-approaches–00

Sergey Slovetskiy
IETF93 - Prague

Background

- At IETF 92 in Dallas, we agreed to look at HTTPS traffic delegation
- Concluded that there was a problem and an interest
- Next steps
  - Write an internet-draft
  - Reach out to the list to invite interested people
  - Have I-D discuss problems and potentials solutions

Use Case(s)

- Start with simple basic Use Case:
  - User Agent request is redirected from Origin CSP (Content Service Provider) to CDN surrogate
- Expand to classic CDNI Use Case:
  - uCDN is delegating delivery of encrypted traffic (HTTPS) to a dCDN
- Map to request routing mechanisms:
  - DNS-based
  - HTTP-based
  - URI rewriting
  - …
- HTTP version:
  - HTTP 1.1 now
  - HTTP/2 in the future (e.g. alt-svc)?

Houston, we have a problem...

- Or do we really?
  - Assumption: "Request redirects do not (always?) work over TLS"
- Lets' explore:
  - HTTP to HTTPS is NOT OK
  - HTTPS to HTTPS: seems OK but… is it enough? See e.g. [1]:

    *"**Problems with the certificate model** appear to be more challenging, including among others: design and implementation issues in the CA/Browser (CA/B) trust model leading to fragility (compromise of a single CA can, at least temporarily, undermine system-wide security) and **lack of trust agility**, **poor support for certificate revocation**, a **reduction in CA diligence in certificate issuance**, and **user interface challenges** related to reliably signalling to end-users, in ways not ignored or spoofed, security indicators and site authentication information."*
  - DNS-based is NOT OK [2]

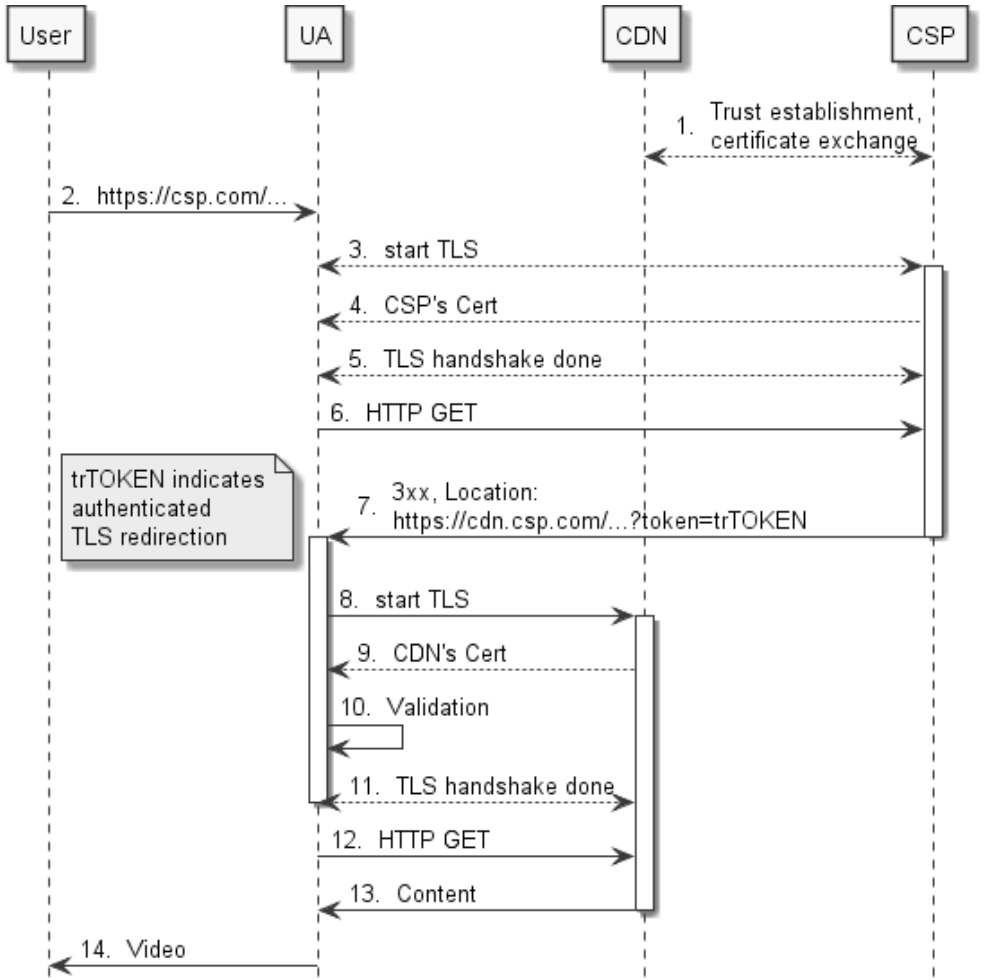
© NASA - http://history.nasa.gov/SP-350/i13-1.jpg

[1]: J. Clark and P. C. van Oorschot, "SoK: SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements," , 2013 IEEE Symp. on Security and Privacy

[2] J. Liang, J. Jiang, H. Duan, K. Li, T. Wan, and J. Wu, "When HTTPS Meets CDN: A Case of Authentication in Delegated Service," , 2014 IEEE Symposium on Security and Privacy

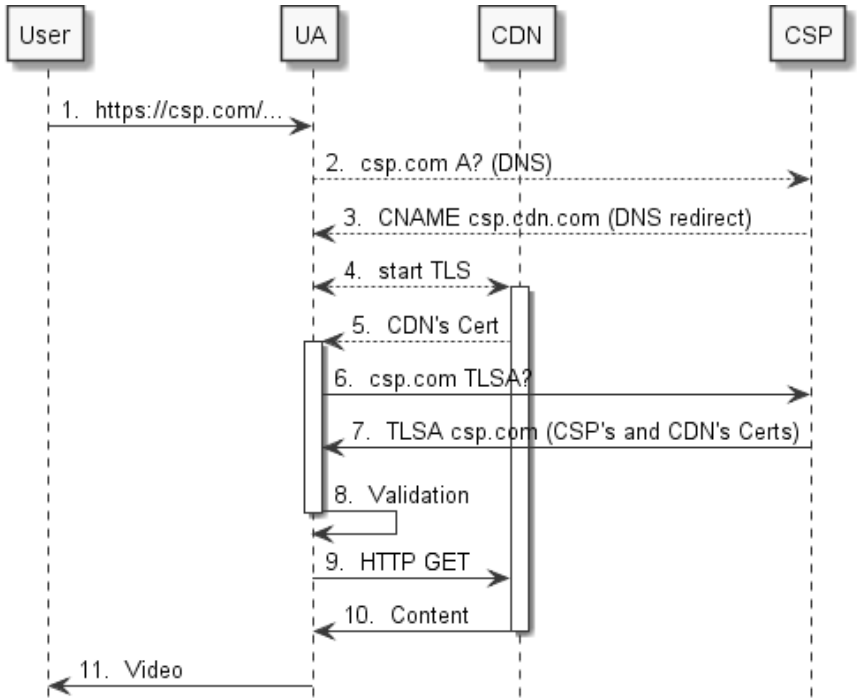
Solution Strawman: HTTPS-based Redirection

- Let's pass the Token:
  - Token binds CSP's and CDN's certificates
  - Signed by CSP
  - Signals "hardened" redirect to UA
  - UA validates
  - Synergies with URI Signing



Solution Strawman: DNS-based Redirection

- Example from [1] using DANE
  - CSP binds its certificate with CDN certificate in TLSA record
  - Additional DNS query
  - UA validates
  - Infrastructure requirement: DNSSEC and DANE



[1] J. Liang, J. Jiang, H. Duan, K. Li, T. Wan, and J. Wu, "When HTTPS Meets CDN: A Case of Authentication in Delegated Service," , 2014 IEEE Symposium on Security and Privacy

Conclusion

- Where do we go from here?
  - Additional Use Cases?
  - Additional redirection considerations?
  - Solution mechanisms / proposals?
  - Dependency on UA
  - Dependency on infrastructure
  - Consider HTTP/2?