SVCB for ECH

Bootstrapping TLS Encrypted ClientHello with DNS Service Bindings

Ben Schwartz <ietf@bemasc.net>
Erik Nygren <erik+ietf@nygren.org>
Mike Bishop <mbishop@evequefou.be>

TLS @ IETF 116
https://datatracker.ietf.org/doc/draft-sbn-tls-svcb-ech/

Reminder: SVCB and HTTPS records

- Goal: bootstrap optimal connections from a single DNS query
- “HTTPS” record for HTTP, “SVCB” for everything else.
- In “AliasMode”, it acts like CNAME but can be at the apex
- In “ServiceMode” it is an extensible service description for things like:
  - Supported TLS ALPNs (e.g., HTTP/2 vs. HTTP/3)
  - Port number
  - Encrypted ClientHello configuration
  - IP hints
  - [Oblivious HTTP upgrade hints]
  - [DNS over HTTPS default path template]
  - …

ServiceMode

svc.example.net. 7200 IN HTTPS **2** svc3.example.net. alpn=h3 ech=XYZ...

svc.example.net. 7200 IN HTTPS **3** svc2.example.net. alpn=h2 ech=ABC...

“Please use QUIC to UDP svc3.example.net:443 with this ECHConfigList, or use HTTP/2 to TCP svc2.example.net:8002 with this other ECHConfigList.”

Timeline

- May 2022: draft-ietf-dnsop-svcb-https (SVCB) IESG approved
- August 2022: SVCB returned to DNSOP, edited, re-IESG approved
- March 2023: SVCB is still MISREF on draft-ietf-tls-esni, and is blocking
  - draft-ietf-add-svcb-dns (RFC Ed Queue)
  - draft-ietf-add-ddr (RFC Ed Queue)
  - draft-ietf-ipsecme-add-ike (RFC Ed Queue)
  - draft-ietf-add-dnr (In WGLC)
  - draft-ietf-add-split-horizon-authority (in WGLC)
  - draft-ietf-ohai-svcb-config (Adopted)
  - draft-ietf-dnsop-svcb-dane (Adopted)
  - draft-ietf-tls-wkech* (Adopted)
  - Various active non-adopted drafts

Solution: IESG Round 3

- SVCB draft-12 has been edited to remove all normative dependencies on draft-ietf-tls-esni:
  - The “ech” key is no longer defined or mentioned in this draft. (Its space in the IANA registry is requested to be marked “reserved” for this purpose.)
  - Discussion of how Encrypted ClientHello alters the client’s use of SVCB and Alt-Svc has been removed.
- SVCB draft-12 has been returned to the IESG for approval (again).
- All substantive ECH-related text has been moved from SVCB draft-11 into draft-sbn-tls-svcb-ech-00.

Next steps...

- Seeking adoption of draft-sbn-tls-svcb-ech in the TLS WG.
- Not seeking immediate WGLC – might as well wait for ECH.