~~Using Service Bindings with DANE~~

Using DANE with SVCB and QUIC

draft -02

Ben Schwartz, Robert Evans

DNSOP @ IETF 118

Reminder: Overview

- DANE = DNSSEC + TLSA
- RFC 7671 = DANE
- RFC 7672 = DANE + MX
- RFC 7673 = DANE + SRV
- This draft = DANE + SVCB

Reminder: Basic DANE

```
www.example.com.                 A 192.0.2.1
_443._tcp.www.example.com.       TLSA …
```

Reminder: SVCB + DANE

```
example.com.                     HTTPS 0 xyz.provider.example.
www.example.com.                 CNAME xyz.provider.example.
xyz.provider.example.            HTTPS 1 . alpn=h2,h3 ...
xyz.provider.example.            A     192.0.2.1
```

Where do the TLSA records go? This draft says where:

```
_443._tcp.xyz.provider.example.  TLSA …
_443._quic.xyz.provider.example. TLSA …
```

(Just like SRV.)

Changes in this revision (-02)

- Recommend against relying on DANE’s weird CNAME behavior.
  - DANE tells clients to look for TLSA records using both ends of the CNAME chain. This is pretty weird and maybe we should deprecate it more generally.
- Various tweaks from DNSDIR and SECDIR reviews.
- NEW: Discussion of Unknown Key Share attacks

Unknown Key Share Attacks

- Discussed in draft-barnes-dane-uks (2016) (never adopted or published).
- Proposes various restrictions on DANE, e.g. *“Even when using DANE, TLS clients MUST verify that the certificate presented by the server represents the name they expect to connect to”*.
- These restrictions would exclude some of the deployment models envisaged in this draft.
- This revision adds a paragraph in the security considerations and an Appendix with a more detailed analysis.
- Conclusion: Only HTTP/1.0 and HTTP/0.9 are vulnerable. Recommended not to use them with DANE.

Document status

- Technical content appears to be stable
- Ready for WGLC!