Using SVCB with DANE
or
Where does TLSA go?

draft-rebs-dnsop-svcb-dane-00
Robert Evans & Ben Schwartz

Overview

This draft does two things:

1. Explain how to do DANE with SVCB and HTTPS records
2. Update DANE for use with QUIC

Applicable to

- **DANE authentication of [A]DoT/DoH/DoQ**
- HTTP/3 with DANE generally
- etc.

Why are these in the same draft?

- A key purpose of SVCB is to enable QUIC upgrade
- Outside of HTTP (e.g. DoQ), SVCB is the only standard way to use QUIC.
- QUIC+DANE text is extremely brief

Background

Background: DANE names

- TLSA query: _$PORT._$TRANSPORT.$BASENAME
    - e.g. _443._tcp.www.example.com.
    - This query follows CNAMEs in the usual way
- *With protocols that support explicit transport redirection via DNS MX records, SRV records, or other similar records, the TLSA base domain is based on the redirected transport endpoint rather than the origin domain.*
- *DANE clients MUST send the SNI extension with a HostName value of the base domain of the TLSA RRset.*

Wrinkle 1: CNAME

Implementations failing to find a TLSA record using a base name of the final target of a CNAME expansion SHOULD issue a TLSA query using the original destination name. That is, the preferred TLSA base domain SHOULD be derived from the fully expanded name and, failing that, SHOULD be the initial domain name.

Clients may need to perform two TLSA queries!

Wrinkle 2: MX reference identifiers

If the TLSA base domain was obtained indirectly via a "secure" MX lookup (including any CNAME-expanded name of an MX hostname), then the original next-hop domain used in the MX lookup MUST be included as a second reference identifier. The CNAME-expanded original next-hop domain MUST be included as a third reference identifier if different from the original next-hop domain.

One SNI but multiple reference identifiers!

Wrinkle 3: SRV and SNI

The reference identifiers SHALL include both the service domain name and the SRV target server hostname (e.g., include both "im.example.com" and "xmpp23.hosting.example.net"). The service domain name is still the preferred name for TLS SNI…

The long-term goal of this specification is to settle on TLS certificates that verify the target server hostname rather than the service domain name..

Clients don’t ask for the name that the spec expects!

Contents

DANE + SVCB

Very simple: **Do SVCB, then Do Dane**:

- SVCB produces a list of (TargetName, Transport, Port)
- Treat each tuple as input to basic RFC 7671 DANE

Just like SRV, except

- Only one reference identity (on each attempt)
- CNAMEs are allowed (Wrinkle 1 applies)

Goal: **Clients can treat DANE as a black box**

DANE + QUIC: Updates RFC 6698

Before: *The transport names defined for this protocol are "tcp", "udp", and "sctp".*

After: *The transport names defined for this protocol are "tcp" (TLS over TCP [RFC8446]), "udp" (DTLS [I-D.draft-ietf-tls-dtls13]), "sctp" (TLS over SCTP [RFC3436]), and "quic" (QUIC [RFC9000]).*

Goal: **Disambiguate DTLS and QUIC, sharpen transport name semantics**

Example

```
_dns.dns.example.com. SVCB 0 dns.my-dns-host.net.
dns.my-dns-host.net.  SVCB 1 . alpn=dot,doq
dns.my-dns-host.net.  SVCB 2 . alpn=dot port=443

_853._tcp.dns.my-dns-host.net.  TLSA ...
_853._quic.dns.my-dns-host.net. TLSA ...
_443._tcp.dns.my-dns-host.net.  TLSA ...
```

Seeking Adoption

Any questions?