The SVCB and HTTPS RRs

Service binding and parameter specification via the DNS

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

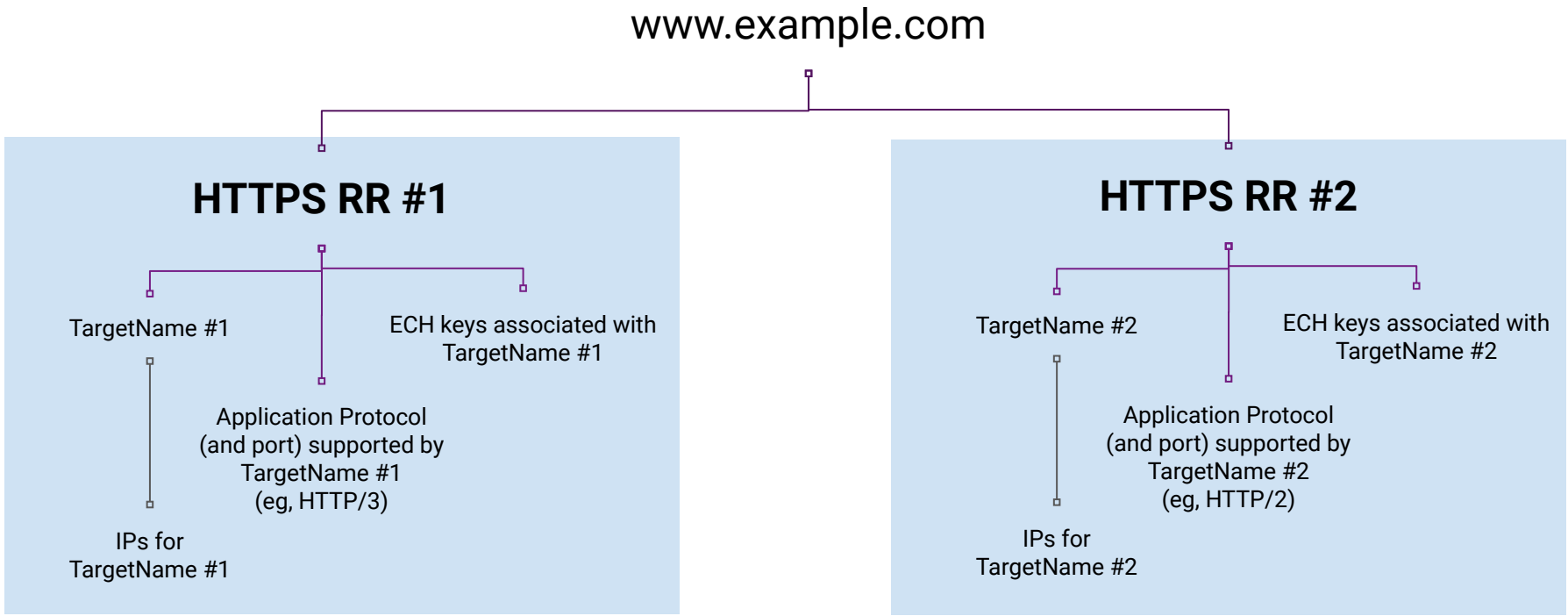
IETF 108 - July 2020
https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-svcb-https-01

SVCB Overview

- Goal: bootstrap optimal connections from a single DNS query
- In “AliasMode”, it enables apex aliasing (only for participating clients)
- In “ServiceMode” it is an extensible service description, currently supporting:
  - TLS ALPN hints
  - Port
  - Encrypted ClientHello configuration
  - IP hints
- “HTTPS” is a SVCB-compatible RR type specialized for HTTPS
  - Indicates origin defaults to HTTPS (similar to “HSTS”)
  - Avoids underscore prefixes
    - Improves compatibility with wildcard domains
    - Compatible with existing CNAME delegations

Example: the HTTPS RR and Multi-CDN hosting

Clients may end up on one or more service endpoints (i.e. sets of servers) which may have different capabilities and keys, such as on different CDNs. The HTTPS RR binds each endpoint together.



AliasMode (SvcPriority=0)

- Covers many “SRV” and “ANAME” use-cases

ServiceMode (SvcPriority>0)

- Covers Encrypted ClientHello use case and other protocol improvements

Lower SvcPriority means preferred

```
svc.example.net.  7200  IN HTTPS 2 svc3.example.net. alpn=h3 port=8003 \
                                                     echconfig=...
```

SvcParams encode protocol, port, ECH keys, and other params

```
svc.example.net.  7200  IN HTTPS 3 svc2.example.net. alpn=h2 port=8002 \
                                                     echconfig=...
```

“Please use QUIC to UDP svc3.example.net:8003 with this ECH configuration, or use HTTP/2 to TCP svc2.example.net:8002 with this other ECH configuration.” (Also, HTTP/1.1 is always supported unless explicitly disclaimed.)

Changes since last meeting (02➜03➜00➜01) (1/2)

- IANA updates
  - SVCB is TYPE64, HTTPS is TYPE65
  - Half of the 16-bit key range is now “first-come-first-served”
- Chain length limit: “there must be a limit, and it must not be zero”.
- New key: “mandatory”.
  - Enables non-backward-compatible extensions without breaking older clients.
- New feature: Alias to “.” means repudiation
  - Same as SRV and “null MX” (RFC 7505)
- Algorithm adjustments from implementer review
  - Client resolution: corrected _attrleaf QNAME instructions, added another fallback option
  - Recursive processing: adjusted normative strength of additional section processing
  - ALPN negotiation: expanded description, simplified client behavior
  - Zone file parsing: corrected ABNF and clarified comma-delimited value parsing

Changes since last meeting (02➜03➜00➜01) (2/2)

- Renames
  - “HTTPSSVC” ➜ “HTTPS” (as suggested by a poll of WG members)
  - SvcDomainName ➜ TargetName
  - SvcFieldPriority ➜ SvcPriority, SvcFieldValue ➜ SvcParams
  - AliasForm/ServiceForm ➜ AliasMode/ServiceMode
  - “origin” ➜ “service”, “service” ➜ “endpoint”, “origin server” ➜ “authority endpoint”
  - Encrypted SNI/esniconfig ➜ Encrypted ClientHello/echconfig
- Clarifications
  - Non-default ports are not changed unless explicitly overridden
  - HSTS applies if any HTTPS RR exists, unless it has unrecognized mandatory keys
  - The HTTPS RR applies to WebSocket, but only the W3C Fetch variant
  - Better text on domain-oriented transport proxies, “affiliated resolvers”, and privacy
  - Better advice on when to use IP hints
  - Text now distinguishes between inner and outer ClientHello with ECH

Next steps...

- Remove TODOs
- Time for WGLC and interop testing!

Current workspace:

https://github.com/MikeBishop/dns-alt-svc

Editor's draft:

https://mikebishop.github.io/dns-alt-svc/draft-ietf-dnsop-svcb-https.html

Thank you to everyone who reviewed the text, filed issues, started implementations, and suggested improvements!