

# HTTPSSVC DNS RR

**HTTPS service location & parameter specification via the DNS**

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

IETF 105 - July 2019

<https://tools.ietf.org/html/draft-nygren-httpbis-httpssvc-03>

# Goals

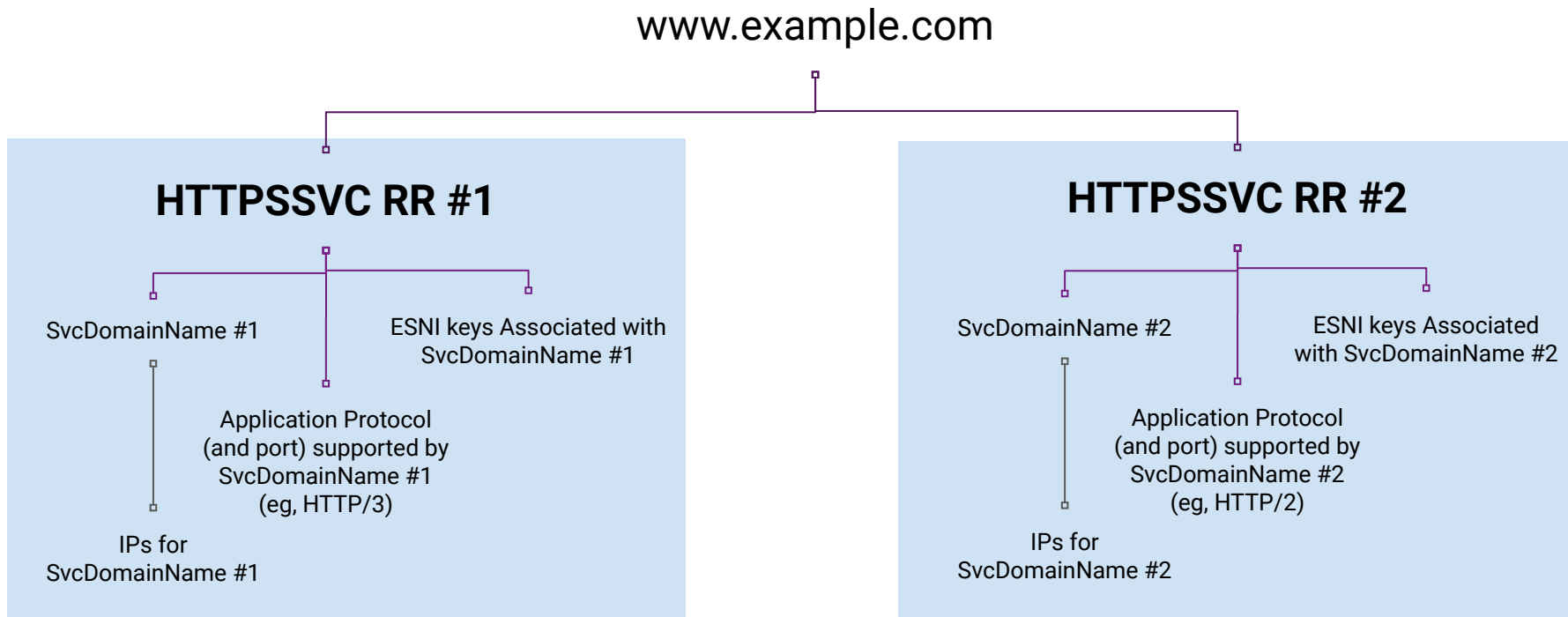
- Solve a number of active problems holistically
- Convey through DNS info needed to make connections to HTTPS URIs:
  - Encrypted SNI keys
  - Transport protocol (HTTP/3, HTTP/2, etc) and associated parameters
  - Indicate origin defaults to HTTPS
  - Service name (similar to SRV) — covers most “ANAME” use-cases
  - ... extensible to future use-cases

## Goals, cont...

- Single new record for browser to resolve in-parallel with AAAA/A
- Design for usability, extensibility, and to enable performance optimizations
- Compelling enough to convince clients (eg, browsers) to implement
- Opportunity to improve secure defaults

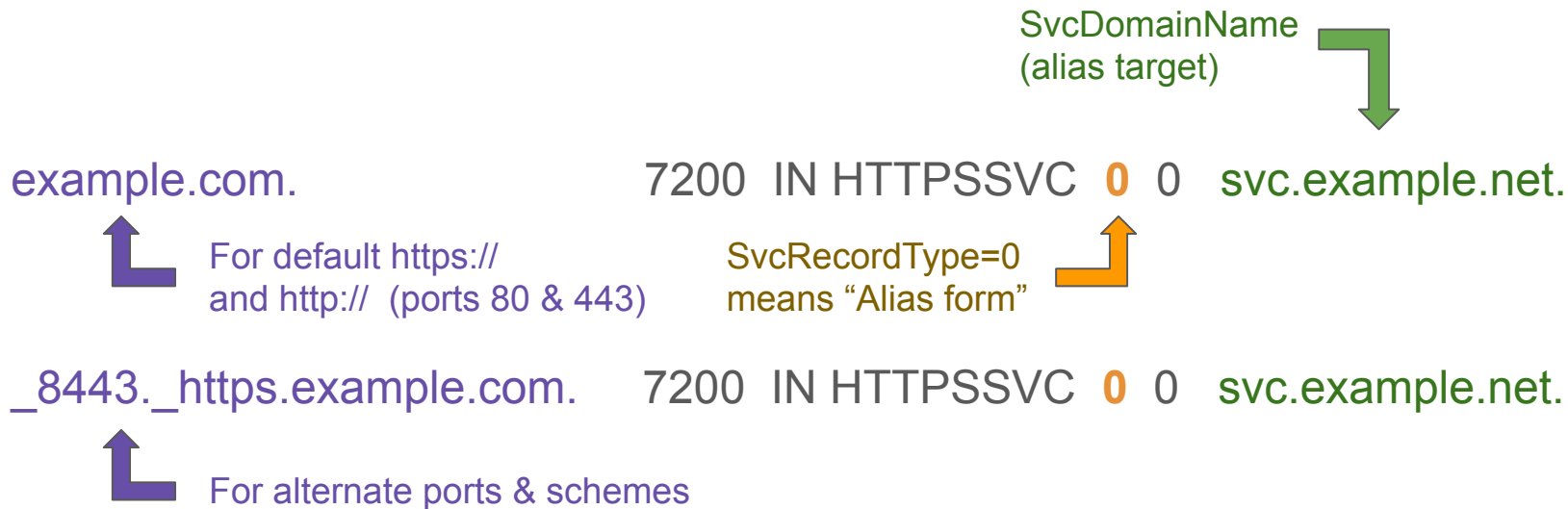
# Associate service endpoints with parameters

*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. HTTPSSVC provides a way to tie these together.*



# Alias form (SvcRecordType=0)

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



# Alternative services form (SvcRecordType=1)

- Covers ESNi use case and other protocol improvements

SvcRecordType=1  
means “Alt-Svc form”



Lower SvcFieldPriority  
means preferred

svc.example.net. 7200 IN HTTPSSVC 1 2 svc3.example.net. "h3=\":8003\"; \\  
esnikeys=\\\"...\\\""

SvcFieldValue encodes protocol, port, ESNi keys,  
and other params in HTTP Alt-Svc (rfc7838) format



svc.example.net. 7200 IN HTTPSSVC 1 3 svc2.example.net. "h2=\":8002\"; \\  
esnikeys=\\\"...\\\""

*“Please use QUIC to UDP svc3.example.net:8003 with these ESNi keys, or use HTTP/2 to TCP svc2.example.net:8002 with these other ESNi keys.”*

# Next steps...

Forums:

- httpbis : on Thursday (best home for adoption?)
- dnsop : on Tuesday (feedback on DNS RR & coverage of ANAME use-case)
- tls : on Thursday (alternative to ESNI RR for HTTPS use-case)

Current workspace prior to adoption:

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

BIND9 private type implementation already available! (Thanks Mark Andrews!)

Feedback on mailing list(s) and to authors most welcome!

# FAQs

- Why HTTP(S)-specific?
  - Different protocols have different bootstrap requirements
  - Builds on Alt-Svc which is a capability already in HTTP
  - HTTP(S) is most common reason given for needing ANAME
  - This proposal is not “browser” specific and should be able to work with API & mobile clients
- Why include ESNI?
  - Specific use-case TLS WG is looking to solve
  - Better for HTTPS use-case than an “ESNI” specific record
  - Easy to split esnikeys=”...” alt-svc parameter to its own draft
- Why address HSTS case?
  - Unique opportunity to improve secure defaults, especially for “bare names”



# Comparison between HTTPSSVC & ANAME

(for the “zone apex CNAME” issue)

## HTTPSSVC

Pros:

- Doesn't require any changes to DNS servers

Cons:

- Only respected by compliant clients
- HTTPS-specific

## ANAME

Pros:

- Doesn't require any changes to clients

Cons:

- Requires complex changes to participating authoritative servers, especially when DNSSEC or ECS is also in use