DNS Transport Signaling

draft-johani-dnsop-transport-signaling-02

Erik Bergström Sara Dickinson Leon Fernandez Philip Homburg Johan Stenstam

Sinodun

NLnet Labs

The Swedish Internet Foundation

November 2, 2025

At The Previous IETF

At IETF123 (Madrid) I presented a previous version of this draft.

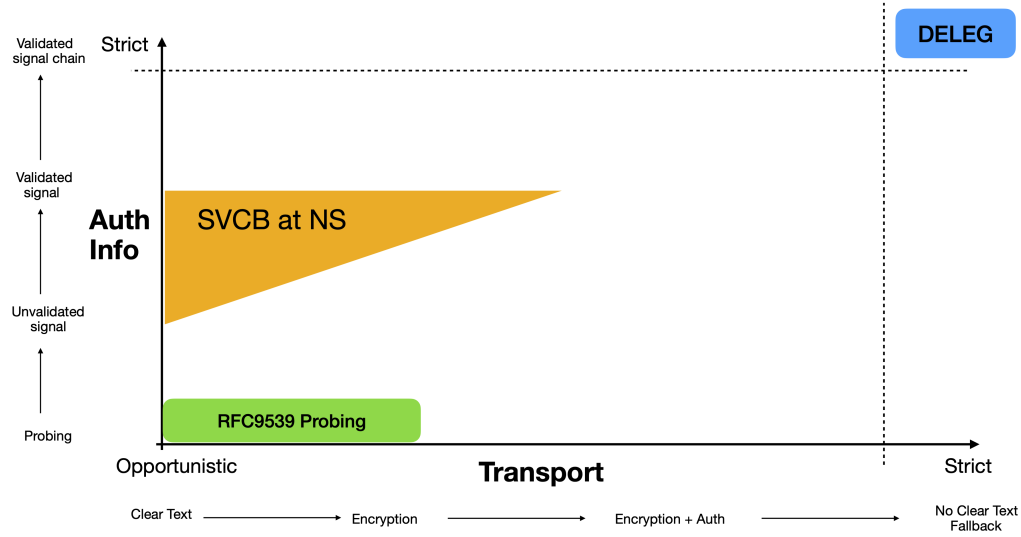
- The focus was on what we now refer to as "opportunistic mode" DNS transport signaling.
- The idea is for the authoritative server to attach an SVCB record to the Additional section of a DNS response.

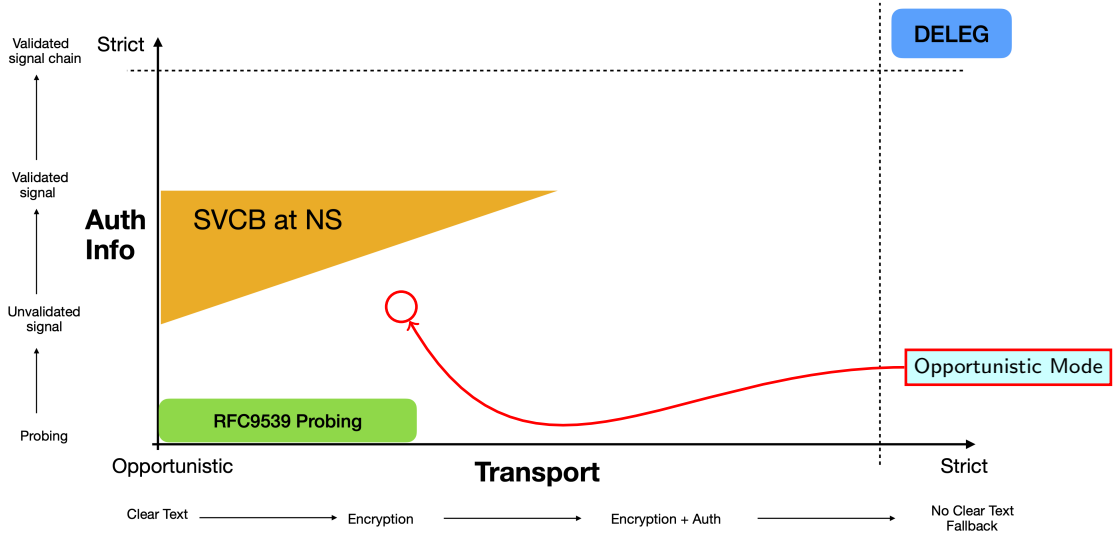
```
_dns.ns.provider.example.  IN  SVCB 1 . (alpn="doq,dot")
```

- The SVCB contains transport signaling that the resolver can then choose to act on or not.

There are various advantages to doing this:

- Ability to distinguish between "test" and "production" transport.
- Ability to upgrade the reliability of the signal.
- Gaining experience with DNS transport signaling prior to the deployment of DELEG.


Validated signal chain
Validated signal
Unvalidated signal
Probing
Strict
DELEG
Auth Info
SVCB at NS
RFC9539 Probing
Opportunistic
Transport
Strict
Clear Text
Encryption
Encryption + Auth
No Clear Text Fallback


Validated signal chain
Validated signal
Unvalidated signal
Probing
Strict
DELEG
Auth Info
SVCB at NS
RFC9539 Probing
Opportunistic Mode
Opportunistic
Transport
Strict
Clear Text
Encryption
Encryption + Auth
No Clear Text Fallback

Addition of "Validated Mode"

We've had a large amount of feedback and we've come to realize a bunch of things:

- While the opportunistic mode was and is a good idea, it is not the only alternative.
- There are other signals that would be useful to have. But a "dangerous" signal cannot be trusted, unless validated.
- It would be good to be able to provide a **validated, secure** signal.

This boils down to, in addition to the opportunistic mode, there is now also what we call "**validated mode**".

- For validated mode to be possible, the `SVCB` record must be DNSSEC-signed.
- Usually, validated mode will require a direct query for the `SVCB` record to the authoritative server.

Addition of the "-do53" Transport Signal

Today, all authoritative servers support DNS-over-UDP/TCP transport.

- I.e. the `alpn="doq,dot,..."` signal is about **additions** to the "default".
- But in the future this will not always be the case (even today it is not always the case).
- We need a mechanism to signal not only additions to the "default" transport, but also removals.

Presence of `alpn="-do53"` in the SVCB record signals that the server doesn't support DNS-over-UDP/TCP transport.

- Among the use cases is the ability to separate more resource intensive transports (DoQ, DoT) from the "default" transport (UDP/TCP).

Other Signals Possible in Validated Mode

With a validated signaling mechanism it is possible to use other signals:

- Validated address records for the authoritative server.
- A validated TLSA RR to verify the certificate of the authoritative server.
- etc.

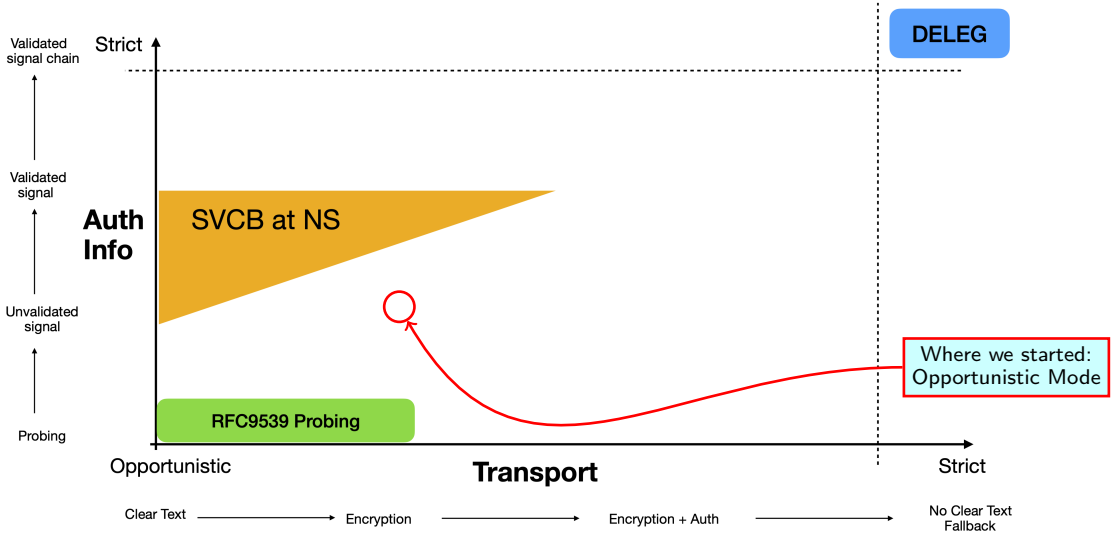
Whether all these signals are put into a single SVCB record:

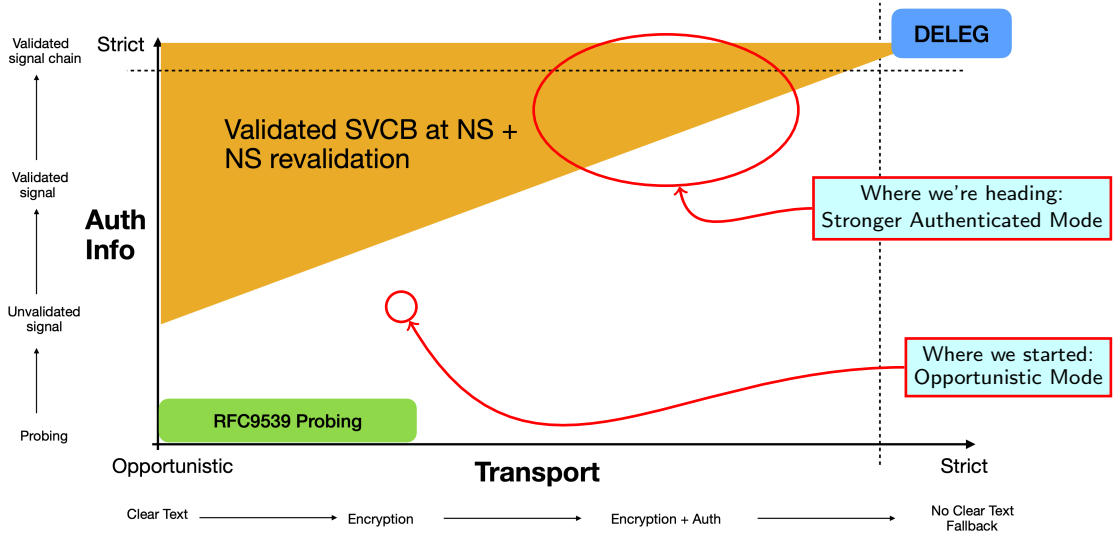
```
_dns.ns.provider.example.  IN  SVCB 1 . (alpn="doq,dot,-do53"
                                    ipv4hint=1.2.3.4 ipv6hint=...  tlsa=...)
_dns.ns.provider.example.  IN  RRSIG SVCB ...
```

. . . or remain in separate records is essentially a matter of choice.

At this point it becomes quite obvious that there is a noticeable similarity to some of the aims of the NS revalidation proposal, `draft-ietf-dnsop-ns-revalidation-11`.

- In the next iteration of this proposal we will try to align terminology and overlapping aims with the NS revalidation proposal.


Validated signal chain
Validated signal
Unvalidated signal
Probing
Strict
DELEG
Auth Info
SVCB at NS
RFC9539 Probing
Where we started: Opportunistic Mode
Opportunistic
Transport
Strict
Clear Text
Encryption
Encryption + Auth
No Clear Text Fallback


Validated signal chain
Validated signal
Unvalidated signal
Probing
Strict
Auth Info
Validated SVCB at NS + NS revalidation
DELEG
Where we're heading: Stronger Authenticated Mode
Where we started: Opportunistic Mode
RFC9539 Probing
Opportunistic
Transport
Strict
Clear Text
Encryption
Encryption + Auth
No Clear Text Fallback

Questions?

Thank You & Contact Information

erik.bergstrom
leon.fernandez
johan.stenstam
@internetstiftelsen.se

sara@sinodun.com

philip@nlnetlabs.nl

Source code https://github.com/johanix/tdns