"DELEG"
What does it mean for DNSSEC?

Petr Špaček

2025-06-09

pspacek@isc.org

Work in progress

- IETF working group DELEG

IETF 118 hackaton: wild idea fair

What would you improve in DNS **if you could**?

- i'd not keep the records separated like NS+DS. One record should contain the NS name, address, capabilities, TLS… And if there are multiple those, each NS can have different capabilities and properties.
- Nameserver-specific DS (allows easy multi-signer: each NS can have independent DNSKEYs)
- Transport should be QUIC. Clients get session tickets and use them when needed. Do53 is used for priming/discovery towards an auto discovery address.
- Auto configure on local networks (multiple responders possible (routers/tunnel-providers/IoT gateways) - verification of functionality)
- Signed ADoT bootstrap on the parent side + EPP extensions to populate it
- main concern - protocol inflexibility
- Much improved
- Delegation has i
- simpler to operat
- No name compre
- Using QUIC allo
- and is signed (o
- I don't like Do53
- Zone Cuts. We n SVCB type record would help here
- If you have a bet
- Get rid of sectio
- DNS text & wire
- Some way to as ple", "I am not authoritative for case of "the name you asked about g info in authority section".
- Proper delegatio
- currently, un-signed NS + glue + signed DS is a mess
- Maybe structured as a DS2/NS2 record that provides
- Secure Delegation (especially to secure transport servers) needs to come from the parents during delegation. Child information on this (NS/DS) is irrelevant.
- SVCB-DNS and maybe TLSA bootstrap info for ADoT
- the *key thoughts* of how to improve/rebuild DNS is always how to handle *delegations*
- the new delegation record signaling DNS2.0 capability of the delegated nameserver has to be able to put into DNS1.0 zone, similarly to DS
- Local network transport can be TLS by stub resolvers.
- CBOR / or otherwise self-describing encoding of messages
- Post-quantum DNSSEC
- we need a delegation record that handles delegated names, addresses, child NS capabilities, TLS certs, eventually DS
- possibly (a clone of) SVCB?
- …

7 pages

Underlying problem

- Lack of extensibility
  - at DNS **delegation point**
- Long version
  - [video]
  - [slides]

Delegation today

```
dom                NS    nameserver1.dom
nameserver1.dom AAAA 3fff::1
```

- No signature
  - Leap of faith
- Not extensible at all

```
dom     DS        1234 99 2 ABCDABCD…
dom     RRSIG     DS …
```

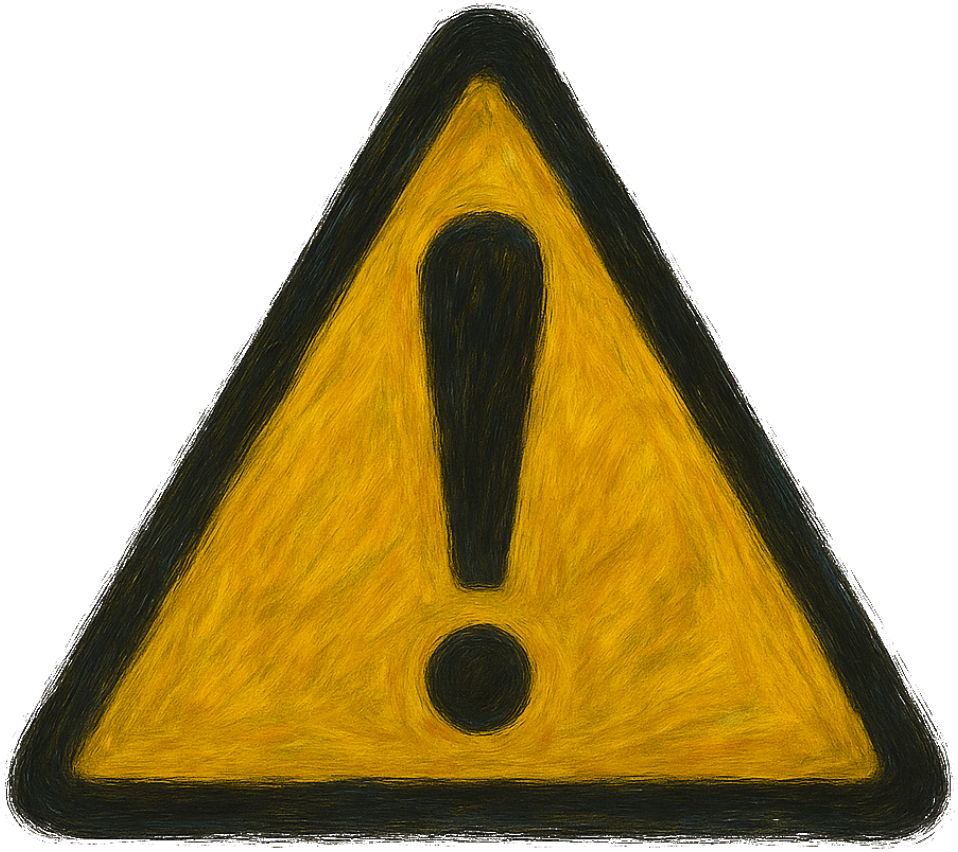
- Not extensible (w/o terrible hacks)

DELEG: Design principles

- DNS won't change – from outside
- Keep
  - **name space**
  - **zones** – management boundaries
  - **stub resolver** model
    - (name, [class,] type) ⇒ records
- **MUST** keep interoperability with the current DNS
  - … and allow incremental evolution

Work in progress

- IETF draft
- draft-ietf-deleg-00
- version **00**!



DELEG modes

- DIRECT
  - Replacement for today's NS + glue records
- INCLUDE
  - Indirection
  - DNSSEC …

DELEG – DIRECT mode

```
example. DELEG DIRECT ( ns1.example.
    Glue6=3fff::1 )
example. RRSIG DELEG …
```

- Parent-side only
  - Eliminates parent/child mismatches
  - Parent signs (same as DS)

```
example.        NS    ns1.example.
ns1.example.  AAAA 3fff::1
```

DELEG – DIRECT mode

```
example. DELEG DIRECT ( ns1.example.
    Glue6=3fff::1 Transport=dot )
```

- Key=value extensibility
- Transport=dot – does not exist yet!

```
example. RRSIG DELEG …
example.      NS   ns1.example.
ns1.example. AAAA 3fff::1
```

DELEG – INCLUDE mode

```
dom DELEG INCLUDE cfg1.operator1.test.
dom DELEG INCLUDE cfg5.operator2.test.
```

```
cfg1.operator1.test (
SVCB 1
ns1 transport=do53 )
```

```
cfg5.operator2.test. (
SVCB 1
ns5 transport=dot )
```

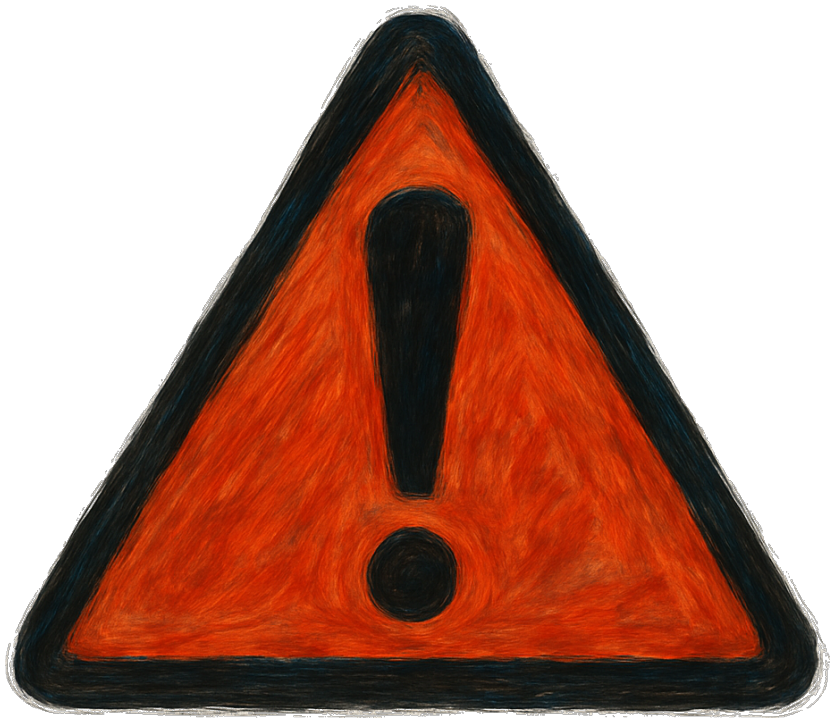
DELEG INCLUDE

- Avoids NS record copy&paste / update problem
- Domain holder
  - **Points to** Operator(s)
- Operator
  - Controls **its own** 'technical parameters'
  - Has no influence over delegation

DELEG
&
DNSSEC

Where is it?

DNSSEC – Where is it?



- **NOT** in draft-ietf-deleg-00
- Very early discussions
- Proposals
  - DNSKEYINCLUDE
  - draft-homburg-deleg-incremental-dnssec-00
  - more ideas in the making …

DNSSEC – Rough idea

- **Optional** indirection for DS/DNSKEY
- Explicit signal that the domain holder **trusts** specific operator(s)

DNSSEC – Indirection concept

```
dom1 DELEG INCLUDE cfg1.oper1.test. trust=yes
dom2 DELEG INCLUDE cfg1.oper1.test. trust=yes
```

```
cfg1.oper1.test. SVCB 1 (
  ns1 dnskey=key.oper1.test. )
```

```
key.oper1.test. DNSKEY 257 3 8 AwEAAa …
```

DELEG & DNSSEC

- Operator **can** be authorized to manage keys
- No need to
  - Update DS RR in the parent
  - Involve domain holder
- Multiple signers/operators
  - No coordination needed
- Same security as 'CNAME' has today

DELEG & DNSSEC

- None of this exists!
- Great interest in the WG

Join us

- IETF DNS Delegation ("deleg") Working Group
  - https://datatracker.ietf.org/group/deleg/about/
- Subscribe to mailing list!
  - https://www.ietf.org/mailman/listinfo/dd
- Draft
  - https://datatracker.ietf.org/doc/draft-ietf-deleg/
- Interim meeting: 2025 **June 17, 1500-1700 UTC**
  - https://mailarchive.ietf.org/arch/msg/dd/NzjOj1lWqXG-eXMmb_CozHf_JuI/

Thank you!

- [slides]: https://datatracker.ietf.org/meeting/118/materials/slides-118-dnsop-hackaton-118-deleg-rr-proposal-00
- [video]: https://youtu.be/7qJ9eg4UREk?t=304
- Main website: https://www.isc.org
- Presentations: https://www.isc.org/presentations