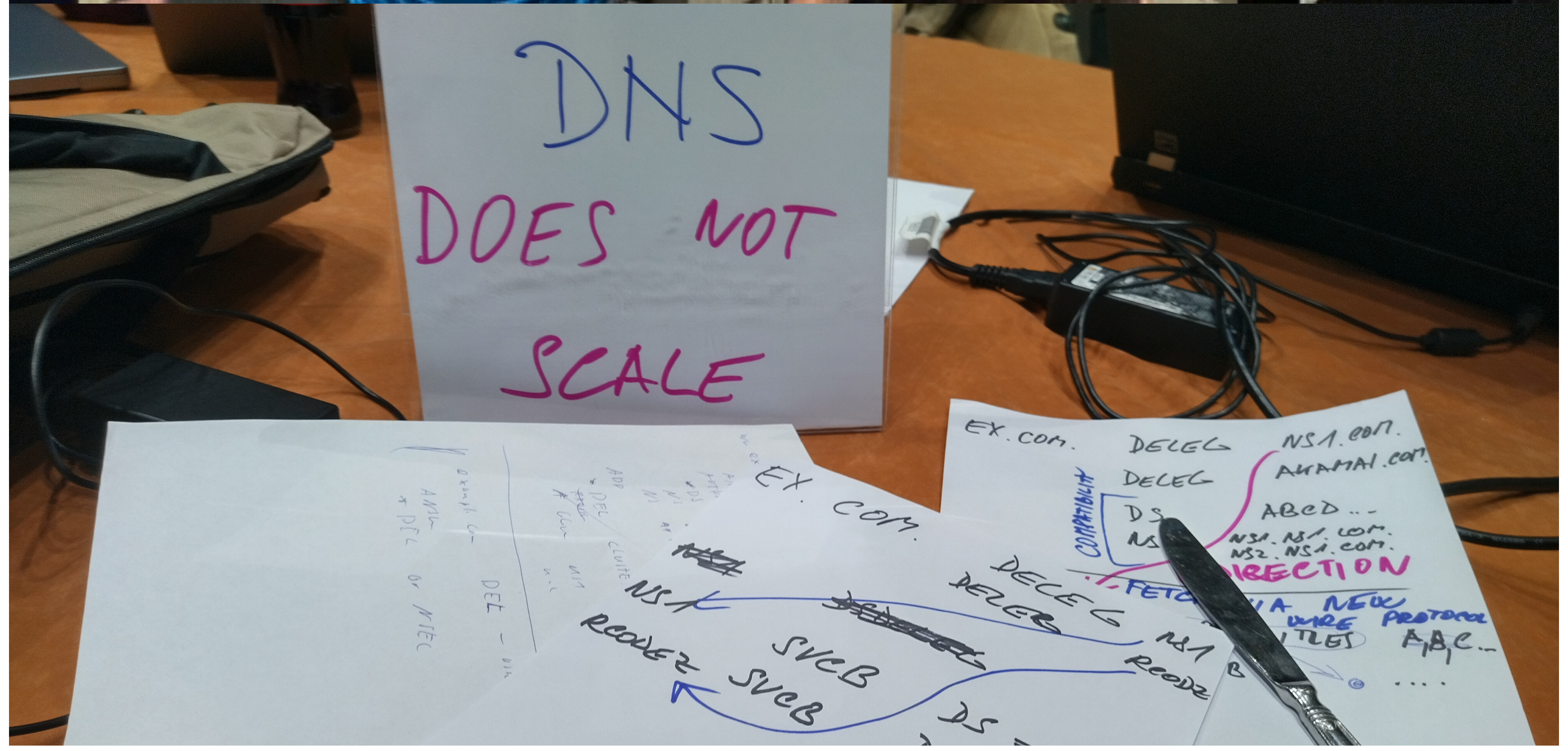
Evoling DNS with DELEG

Ralf Weber (Akamai)

How it started

- Project for the IETF118 (Prague) hackathon
- Around 16 people from various stakeholders met
- After two days came up with the idea for DELEG
  - Parent side SVCB type record
    - Can be signed
    - Has additional data
    - Allows indirection
- Discovered it was similar to Tim Aprils NS2 draft
- Used that as basis for the draft
- Before draft discussions were public
  - DNS-OARC Mattermost chate
  - Github



IETF proceedings

- We presented draft-wesplaap-deleg to the dnsop working group at IETF118
- That lead to an interim meeting of the working group
    - During that meeting it was decided that the work has to happen in its own working group as this might be to big for dnsop
- The BOF for the deleg working group happened at IETF119 in Brisbane
- The deleg working group was approved and met first at IET120 in Vancouver
    - Chairs:
        - Brian Haberman
        - Duane Wessels

Current deleg wg status

- One adopted document (the requirements draft)
  - draft-ietf-deleg-requirements-00
- Two related documents (two slightly different solutions)
  - draft-wesplaap-deleg (the original deleg draft)
  - draft-homburg-deleg-incremental-deleg-00 (different approach using _deleg labels)
- Working group will hold an interim meeting on the requirements draft
  - Tuesday 2024-10-08 15:00-17:00 UTC

Requirements

- Allow future innovation
- Solves current problems (Encryption to auth, DNS operator problem)
- Is compatible with the current DNS (allows gradual deployment)
- Keeps known DNS properties
  - Name space
  - Management boundaries (zones)
  - Registry/Registrar model
  - Data structure (name, [class,] type) -> value

What is DELEG (for me)

- **A parent side only SVCB style record**
- **Why parent side only**
  - Creates a zone cut like NS
  - No ambiguity unlike NS
  - Signed with the parent key like DS
  - Discoverable during normal iterative processing
- **Why SVCB style**
  - Allows additional parameters
  - Allows indirection
  - All delegation information can be signed

```
In Domain/Direct
Old:
example.com.  86400  IN NS     ns1.example.com.
ns1.example.com.    86400   IN  A  192.0.2.1
ns1.example.com     86400   IN  AAAA    2001:DB8::1

New:
example.com.  86400  IN DELEG  1 ns1.example.com. (
               ipv4hint=192.0.2.1
               ipv6hint=2001:DB8::1 )



Out of Domain/Indirect
Old:
example.com.  86400  IN NS      ns2.example.net.

New:
example.com.  86400  IN DELEG 0 config2.example.net.

New delegated to zone:
config2.example.net 3600    IN SVCB . (
     ipv4hint=192.0.2.54,192.0.2.56
     ipv6hint=2001:db8:2423::3,2001:db8:2423::4 )
```

What needs to change

- For legacy aka current DNS
    - Nothing needs to change it will just work
    - This was tested by Roy Arends and Shumon Huque
- For modern DNS to use DELEG
    - DNS software needs to understand the DELEG resource record
    - Authoritative servers need to provide DELEG with or instead (when signalled) of NS, DS for referrals
    - Authoritative servers that have both child and parent need to answer from the parent for a direct DELEG query (similar to DS)
    - Zone owners need to signal DELEG support (DNSKEY flag)
    - Resolvers need to use DELEG records in referrals

Questions