

New DELEGation for registries

Petr Špaček

2024-02-27

pspacek@isc.org



Delegation today (1987 – 2024)

Delegation today: out of bailiwick

```
$ dig @a.ns.nic.cz example.cz. NS
```

```
example.cz. NS ns1.he.net.
```

```
example.cz. NS ns2.he.net.
```

```
example.cz. NS ns3.he.net.
```

```
example.cz. DS ...
```

Name Server **set**

equivalent servers

Delegation today: out of bailiwick

```
$ dig @a.ns.nic.cz example.cz. NS
```

```
example.cz. NS ns1.he.net.  
example.cz. NS ns2.he.net.  
example.cz. NS ns3.he.net.  
example.cz. DS ...
```

- server name
- implies port 53
- no encryption
- not extensible
- not signed

Delegation today: child side

```
$ dig @ns1.he.net. example.cz. NS
```

```
example.cz. NS ns1.he.net.
```

```
example.cz. NS ns8.he.net.
```

```
example.cz. NS ns9.he.net.
```

- no consistency guarantees
- ambiguity
- resolver implementations differ

Delegation today: out of bailiwick

```
$ dig @a.ns.nic.cz example.cz. NS
```

```
example.cz. NS ns1.he.net.  
example.cz. NS ns2.he.net.  
example.cz. NS ns3.he.net.  
example.cz. DS ...
```

DNS operator

DNS operators today

- Not expressed in DNS
 - People can guess
 - Not machine readable
- Data update is hard
- Multiple operators ...

DNS operators today

- "The letter **O** in RRR stands for Operator"



Foto:
[Extra medium](#)

LOOK!
THE LOCH NESS
MONSTER!

Delegation today: in-bailiwick

```
$ dig @a.ns.nic.cz nic.cz. NS
nic.cz. NS a.ns.nic.cz.
nic.cz. NS b.ns.nic.cz.
nic.cz DS ... "glue"
```

```
a.ns.nic.cz. A 194.0.12.1
a.ns.nic.cz. AAAA 2001:678:f::1
b.ns.nic.cz. A 194.0.13.1
b.ns.nic.cz. AAAA 2001:678:10::1
```

Future DNS



DELEG proposal

- Work-in-progress
- Very early stage
- Focus on concepts
 - Details **will** change



DELEG proposal: reading

- DNS part – DNS-OARC 42 [presentation](#)
- DNS protocol - draft on [Github](#)
 - Three parts
 - DELEG mechanism
 - Encrypted transports
 - DNSSEC
- [EPP draft](#)

DELEG proposal: Principles

- **Do not** change NS delegation mechanism
- Add new extensible mechanism
- Coherent namespace
 - Same registrant controls
 - old NS
 - new DELEGations

DELEG: Goals

- Simplify maintenance
 - **Operators own** technical information
 - NS set
 - DS set (DNSSEC)
 - Future extensions
 - TTL @ operator zone
 - Eliminate registrant confusion
 - Copy & paste errors
- Enable DNS extensions

DELEG: ALIAS mode

- Registry side

```
example.cz. NS ...  
example.cz. DELEG 0 set9.cloudflare.com.  
example.cz. DELEG 0 nssetX.he.net.
```

delegation **to an operator** (or more!)

- Operator side

```
nssetX.he.net. SVCB 1 ns1.he.net.  
nssetX.he.net. SVCB 1 ns2.he.net.
```

DELEG
equivalent
of a NS set

DELEG: ALIAS mode

- Registrant configures
 - single name (per operator)
- Registrant does **not** touch
 - individual server names
 - DS records (DNSSEC)
- Short TTL @ operator side
- Smaller error rate

DELEG: Operator managed params

- nssetX.he.net. SVCB 1 ns1.he.net.
nssetX.he.net. SVCB 1 ns2.he.net.
nssetX.he.net. SVCB 1 ns-dot.he.net. alpn=dot
nssetX.he.net. SVCB 1 (ns-doq.he.net. alpn=doq
ds="12345 ABCDEF...")

- Operator in charge

Extensibility!

- Technical params – inside operator's zone
- TTL

DELEG: DIRECT mode

- Registry side only
- In-bailiwick setup

```
example.cz. NS ...
example.cz. DELEG 1 ns1.example.cz. (
    ipv4hint=192.0.2.1
    ipv6hint=2001:db8::1
    alpn=dot
)
```

DELEG: Open question

- NS and DELEG technically independent
 - On DNS level
 - Legacy NS & DS for compatibility
- Registry policy
 - Auto-generate NS & DS out of DELEG (ALIAS mode)?
 - If not – DNS extensibility still works
- EPP draft

DELEG proposal: Contribute!

- IETF dd mailing list ← contribute here!
 - <https://www.ietf.org/mailman/listinfo/dd>
- IETF 119 BoF
 - "New DNS Delegation"
 - 2024-03-19 23:30-01:30 UTC
- EPP draft
 - <https://datatracker.ietf.org/doc/draft-brown-epp-deleg/>



Thank you!

- Main website: <https://www.isc.org>
- Software downloads:
<https://www.isc.org/download> or
<https://downloads.isc.org>
- Presentations: <https://www.isc.org/presentations>
- Main GitLab: <https://gitlab.isc.org>

