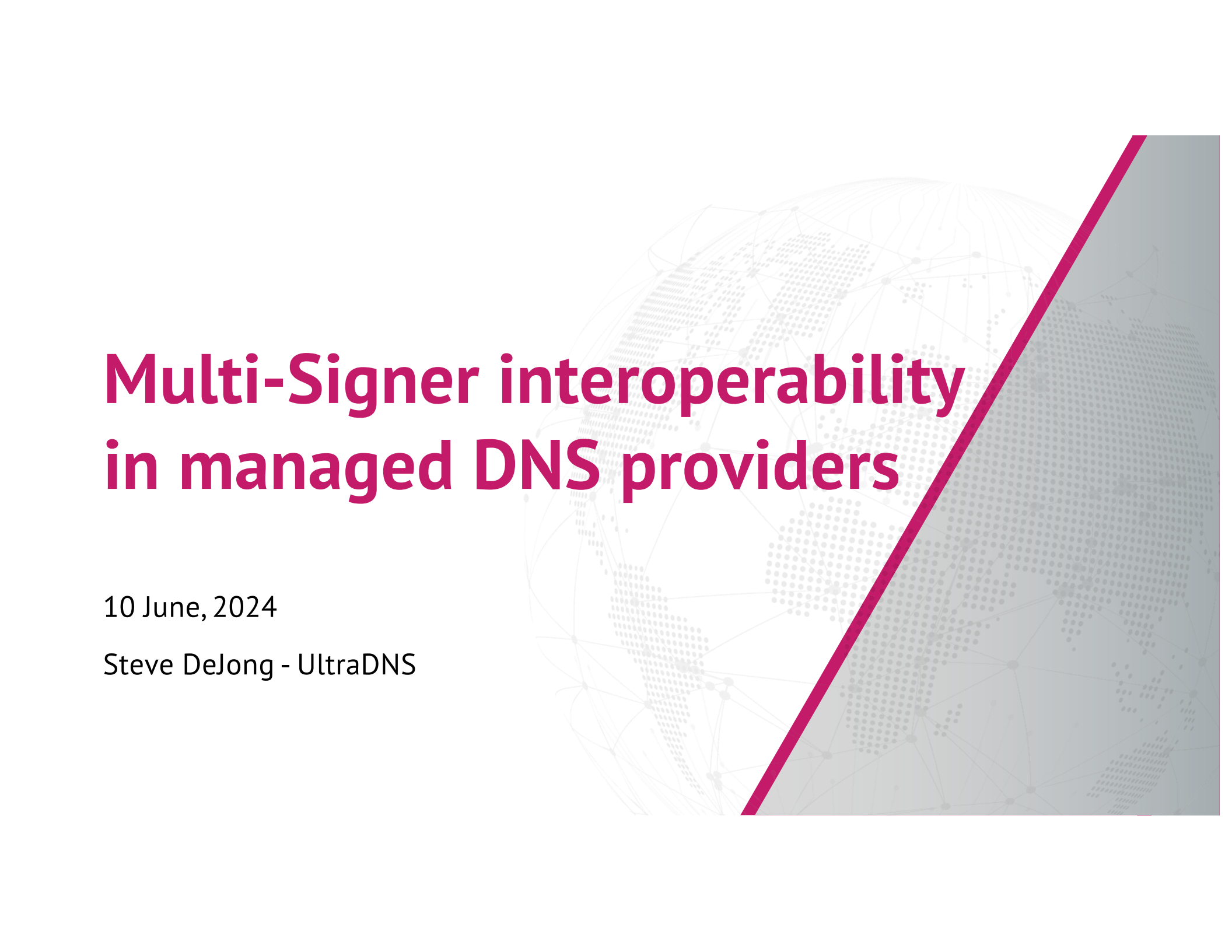




Multi-Signer interoperability in managed DNS providers

10 June, 2024

Steve DeJong - UltraDNS

DNS providers and multi-signer

Many enterprises today employ the service of multiple DNS providers to distribute their authoritative DNS service. Deploying DNSSEC in such an environment may present some challenges, depending on the configuration and feature set in use. [RFC 8901]

Providers have different methods for serving tailored responses

- Responses determined by source geography / network
- Dynamic management of rr-sets
- Representation of apex records

Non-standard or proprietary zone formats for custom features

- Static signing of zones with configured custom features is impractical
- Zone XFR does not work when these features are used

Motivation

Managed DNS providers working together to implement multi-signer DNSSEC [RFC 8901] in real-world environment

- Demonstrate working use cases
- Identify implementation differences between providers
- Identify automation challenges or opportunities to reduce the need for human interaction when signing domains
 - Ability to handle common DNSSEC activities like KSK and ZSK rollovers while maintain the DNSSEC chain-of-trust

Bootstrapping a new domain

Using two independent managed DNS providers, configure a new domain for DNSSEC with multi-signer enabled.

1. Provision the domain on *provider-A* and *provider-B*
2. Register domain with NS delegations from both providers

Bootstrapping a new domain

```
→ ~ > dig @a.gtld-servers.net. ultra8901.com NS +noall +authority
ultra8901.com.      172800  IN      NS      pdns3.ultradns.org.
ultra8901.com.      172800  IN      NS      pdns4.ultradns.org.
ultra8901.com.      172800  IN      NS      pdns1.ultradns.net.
ultra8901.com.      172800  IN      NS      pdns2.ultradns.net.
ultra8901.com.      172800  IN      NS      dns1.p07.nsone.net.
ultra8901.com.      172800  IN      NS      dns2.p07.nsone.net.
ultra8901.com.      172800  IN      NS      dns3.p07.nsone.net.
ultra8901.com.      172800  IN      NS      dns4.p07.nsone.net.
```

provider-A

provider-B

```
→ ~ > dig @64.6.64.6 ultra8901.com NS +short
dns1.p07.nsone.net.
dns2.p07.nsone.net.
dns3.p07.nsone.net.
dns4.p07.nsone.net.
```

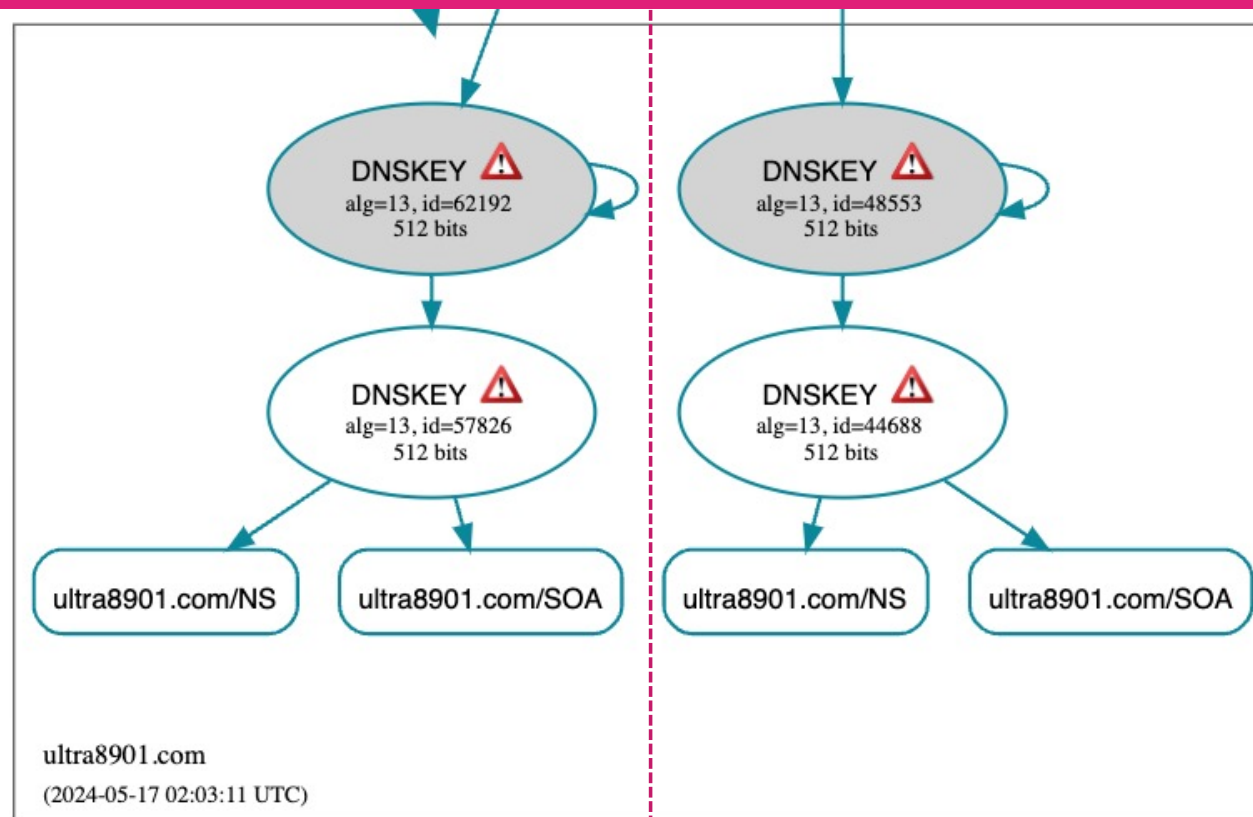
```
→ ~ > dig @8.8.8.8 ultra8901.com NS +short
pdns1.ultradns.net.
pdns2.ultradns.net.
pdns3.ultradns.org.
pdns4.ultradns.org.
```

The NS set you see depends on the authoritative provider

Bootstrapping a new domain

3. Sign the domain at *provider-A*
 - Collect the DS and DNSKEY information generated in the signing
4. Sign the domain at *provider-B*
 - Collect the DS and DNSKEY information generated in the signing
5. Update registration to publish DS from both *provider-A* and *provider-B*

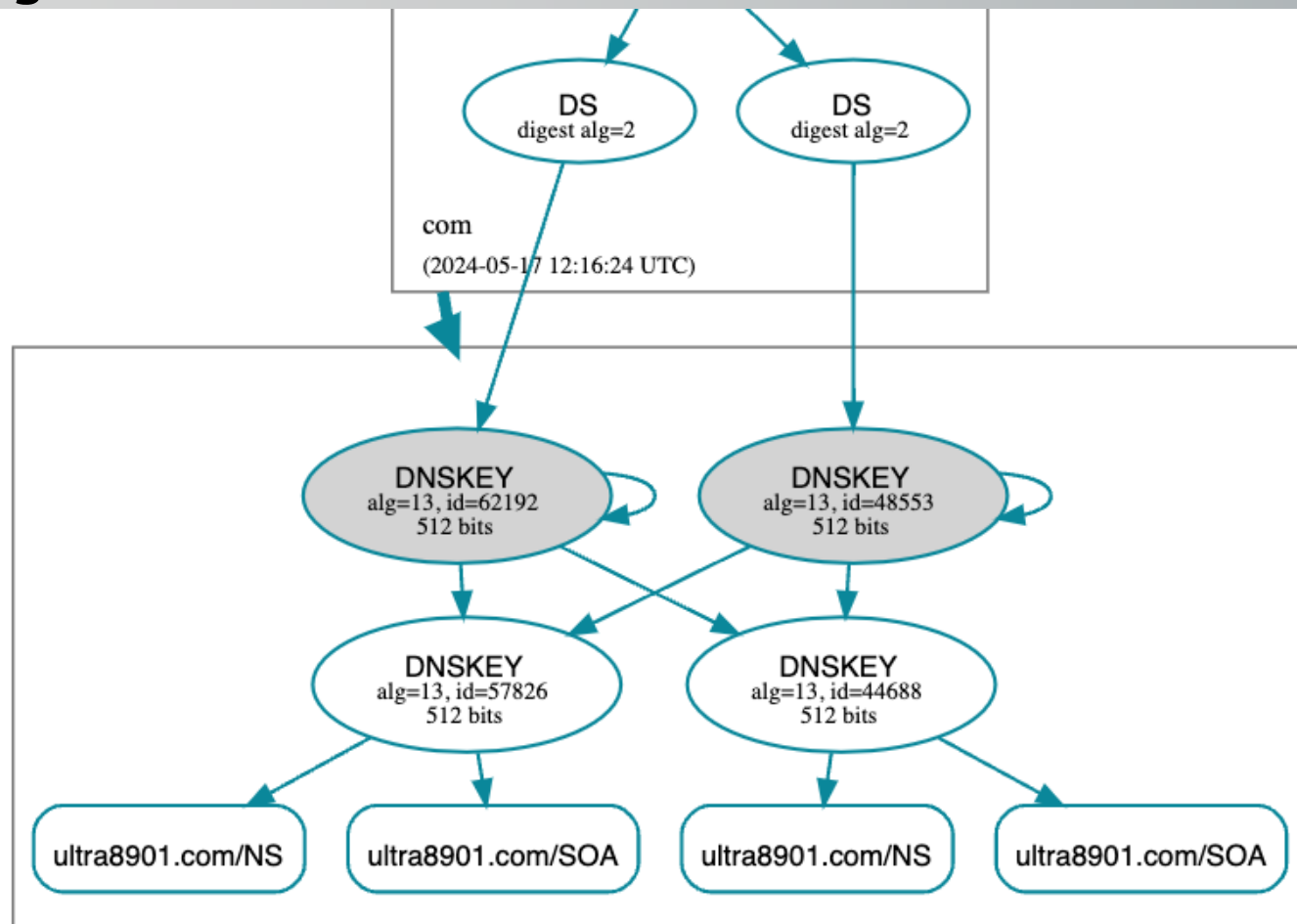
Bootstrapping a new domain



Bootstrapping a new domain

6. Using managed provider API for *provider-A*
 - Add *provider-B* DNSKEY information into *provider-A* domain
7. Using managed provider API for *provider-B*
 - Add *provider-A* DNSKEY information into *provider-B* domain
8. Configure automated handling of signing changes for each provider
 - Handling changes is different for each provider
 - Requires domain owner to write scripts or tools to manage

Bootstrapping a new domain



Discoveries

Key management differences

- KSK
 - Unique to zone vs. shared across many zones
 - Keys may / may not be rotated
- ZSK
 - Keys may / may not be rotated
 - Rotation may / may not be automated
 - Rotation intervals vary
- Customer accessible signing details
 - API commands should be available so that customer/administrator can retrieve DS and DNSKEY signing information

Discoveries

Change notifications are provider dependent

- API authorization and RBAC controls
- API support for managing signing details

Domain owner/administrator capabilities

- Current methods put automation responsibility on the owner
- May not be able to operate signal handling methods necessary

On-going DNS protocol improvements

- DNSSEC automation, bootstrapping, generalized NOTIFY are still in draft
- These will help. Need to be ratified

Thank You

