DNS Provider Coordination of Multi-Signer and DNSSEC Automation

25 October, 2023

Steve DeJong - UltraDNS

Automation of DNSSEC changes in a multi-signer configuration requires some mechanism for coordinating the necessary DNS records between different signers. Managed DNS providers will have different mechanisms for making changes to zone configurations making a single, protocol-based solution impractical.

Recent drafts and work by the DNSSEC-Provisioning project are enabling the automation of DNSSEC management functions including multi-signer functions. This work removes much of the friction and frustration preventing more wide-spread adoption of DNSSEC by domains below the TLD level.

For managed DNS providers managing the configurations of thousands of signed domains there are additional considerations for automating across a wide variety of domains, signers and parents.

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

Multi-signer project has been presenting for a while

- Demonstrations of implementations using common nameservers
- Small scale proofs in controlled environments

UltraDNS began investigating implementation earlier this year

We assumed low adoption

We thought it would be straightforward

We soon realized

- Supporting multi-signer at vendor scale for hundreds of domains across many different DNS operators can be challenging
- DNSSEC adoption and multi-signer support are problems that are screaming for automation

Considerations

Provisioning

- What qualifies a domain to be “ready” for multi-signing
- The details needed for setting up multi-signing

Bootstrapping and un-signing of domains

Transport security when sending / receiving signals

- Where to send signals
- Configuration information for src/dst details
  - ACLs
  - TSIG
  - HTTPS
  - IP addresses

Considerations

Scanning

- Continuous scanning of a large number of multi-signed domains is impractical
  - What frequency of scanning is appropriate/manageable

Timing

- Ensuring that rollovers do not collide or overlap
- ZSK rollover frequency
- How long to wait for other providers before declaring failure

Failure conditions and recovery

- Unable to deliver signals
- Signals are not processed
- Failure to scan
- Scanning detects changes with no signal

Considerations

Troubleshooting

- Enable domain owners to check current DNSSEC details
- Must be able to support and answer customer questions
- check-ds
- On demand scan DNSKEY details in all nameservers

Support for automation

- Centralized or decentralized
- Signal consumer support
- When/where to build a controller

Multi-signer automation models

Owner centralized

- Domain owner is responsible for the synchronization of DNSKEY information between their chosen DNS providers

Vendor centralized

- DNS signers are able to signal each other with DNSKEY change information

Decentralized

- A service that is capable of receiving DNSSEC information from multiple signers and distributing the changes to a variety of consumers

Owner centralized

Domain owner configures domain on each provider.

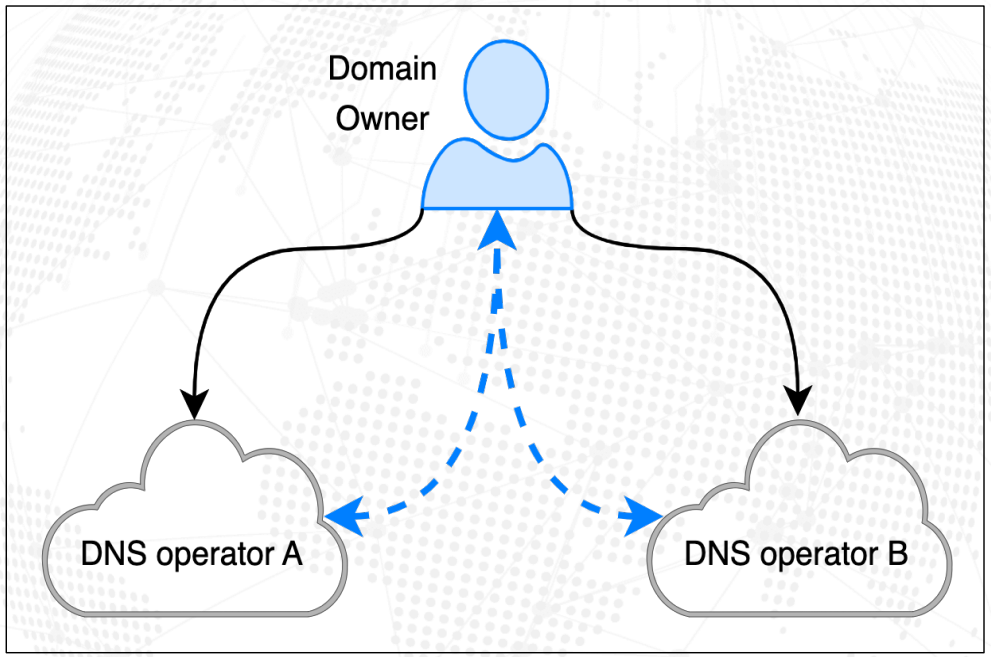
Providers signal owner on changes

- Webhooks or other notifications

Owner responsible for sending details to other providers

Providers scan to ensure complete

- cds-consistency



Owner centralized

✓Domain owner is responsible for synchronization

- Has necessary API credentials for each provider
- Familiar with signaling and notification of each provider

✓Can be (somewhat) automated

- Webhook processing
- Serverless functions

ⓧ Domain owner does may not have capabilities

ⓧ Domain owner still responsible for communicating changes to parent / registrar

ⓧ Failure handling and rollback situations are difficult to address

Vendor centralized

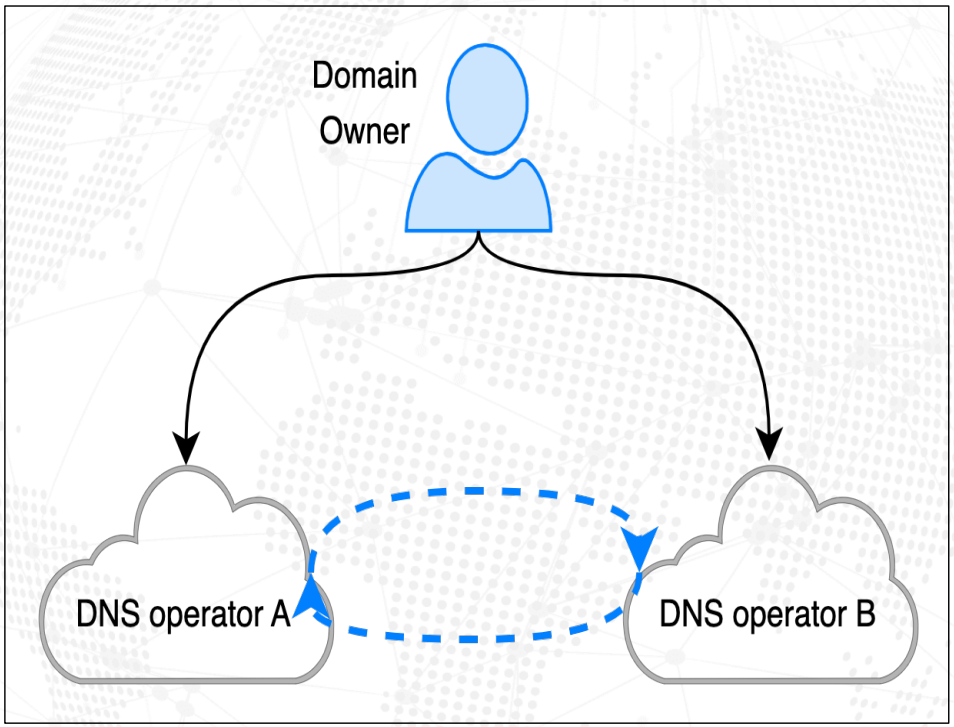
Domain owner configures domain on each provider.

Providers signal each other on changes

- generalized-notify
- Other mutually agreed methods

Providers scan to ensure complete

- cds-consistency



Vendor centralized

✓Does not need to rely on vendor specific API

- CDS/CDNSKEY/CSYNC processing

✓Signaling sent directly to other signers removes operational burden from domain owner

✓Automated key rolls

ⓧ Still undefined cross-vendor signaling methods

- generalized notify not yet ratified
- other methods require cross-vendor agreement

ⓧ Requires secured communication path between vendors

ⓧ Configuration complexity concerns for > 2 signers

ⓧ Bootstrapping, un-signing, failure recovery

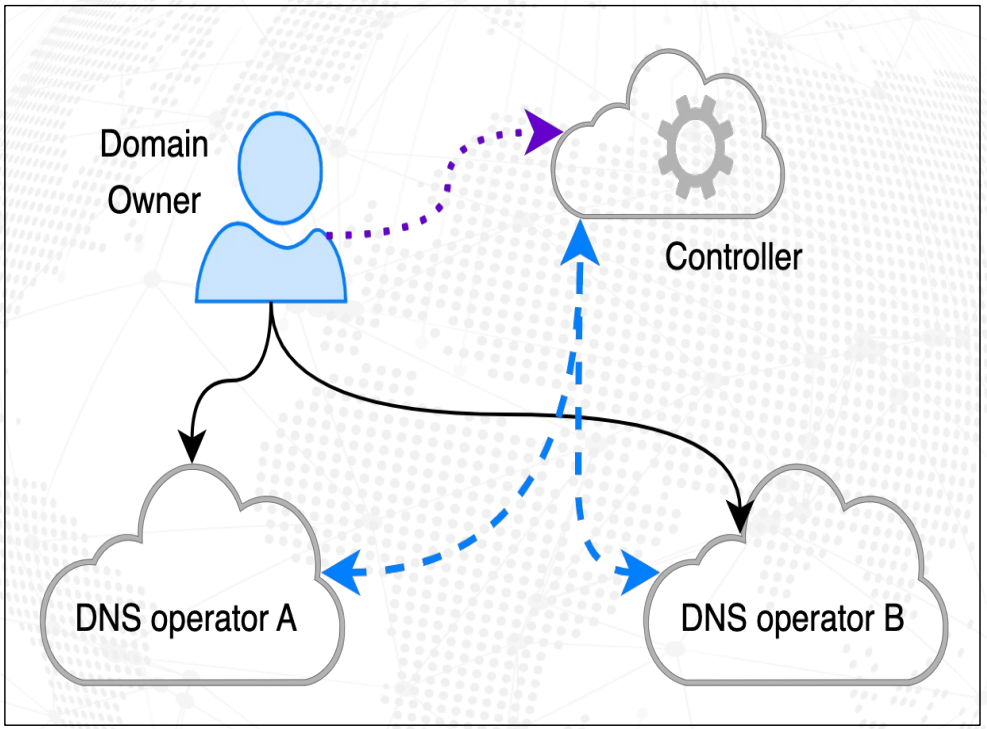
Decentralized

Domain owner configures domain on each provider

Domain owner registers domain with controller

Ensuring consistency can be done by the controller or the DNS operator

Can be easily extended to > 2 operators or parent registrars



Decentralized

✓Does not need to rely on vendor specific API

- CDS/CDNSKEY/CSYNC processing

✓Change events signal a managed set of endpoints

✓Automated key rolls

✓Bootstrapping support

✓Easily extends to parent registrars and registries

ⓧ New service to build and maintain

ⓧ Controller service needs to handle registration of domain owners and signal consumers

ⓧ Undefined deployment models still to be determined

ⓧ Not quite ready for large scale vendor deployments

UltraDNS multi-signer and DNSSEC automation

Support RFC 8901

- Model 2 – unique KSK, ZSK per provider
- Algorithm 13

First generation – Owner centralized – early ‘24

- API based management of external signer DNSKEY
- CDS / CDNSKEY support
- Webhook signaling of key management events
- Scanning system

UltraDNS multi-signer and DNSSEC automation

Second generation – mid ‘24

- generalized-notify capabilities
- Initial implementation of controller service

Third generation - TBD

- Complete controller service
- Registration of domains, producers, consumers

Thank You

RFC 8901 Multi-Signer DNSSEC Models

RFC 7344 Automating DNSSEC Delegation Trust Maintenance

RFC 8078 Managing DS Records from the Parent via CDS/CDNSKEY

draft-ietf-dnsop-dnssec-automation

RFC 6781 DNSSEC Operational Practices

draft-ietf-dnsop-cds-consistency

draft-ietf-dnsop-generalized-notify

draft-ietf-dnsop-dnssec-bootstrapping

Multi-Signer Project

MUSIC