DNS Multi-Provider Requirements

https://github.com/johanix/draft-johani-dnsop-multi-provider-requirements

Speaker: Shumon Huque

Johan Stenstam, Shumon Huque, Peter Thomassen, Steve Crocker, Matthijs Mekking, Philip Homburg, Erik Bergstrom, Steve De Jong, Christian Elmerot, et.al.

ICANN 84

October 29th 2025, Dublin, Ireland.

Introduction

A collaboration group attempting to identify a baseline set of requirements for multi-provider DNS architectures.

Multi-provider deployments increasingly common - high availability, survive failure of any single provider.

But brings complexity, and frequently a set of manual steps to bootstrap and operate, which are error prone, and present operational risk.

Can be for both unsigned and signed zones.

Objective: outline key requirements for developers, implementers, and deployers.

Actors

DNS Provider

Signing Party

Publishing Party

Zone Owner

Scenarios

- Unsigned zone & Multiple Providers serving it.

- Signed zone, Single Signer, Multiple Providers serving it.
  - Signer could be the Zone Owner, or one of the providers. Commonly, Zone Transfer is used to transfer the signed zone to the provider(s).

- Signed zone, Multiple Signers, Multiple Providers serving it.
  - Providers receive an unsigned zone from the zone owner via XFR, then each sign it (bump in the wire style).
  - Zone owner keeps authoritative view of the zone, updates zone identically at via each providers provisioning API.

Coordination & Synchronization

NS set (use CSYNC, Dynamic Update, or API?)

For DNSSEC Multi-Signer, DNSKEY, CDNSKEY, CDS

and key rollover coordination (use Generalized NOTIFY or API hooks?)

What about glue records?

Zone Data synchronization (orthogonal to infrastructure synchronization)

Single source & zone transfers; Update data identically at provider APIs.

Note prior art: with HSYNC, etc.

Remain extensible for the future (DELEG etc)

Onboarding & Offboarding

Mechanisms to bring on new providers, or transition out existing ones.

For multi-signers, a framework is presented in the IETF dnssec-automation draft.

Requirements (Hard & Soft)

Under discussion and debate still ...

Includes: requirements to securely authenticate DNS providers, interfaces to automatically update delegation info in parent, support for update & publication of CSYNC/CDS/CDNSKEY RRsets, key change notifications, ability to smoothly onboard and offboard providers, support for error reporting & notification, keytag collision avoidance, etc.

Continuing & Next Steps

Discussion on IETF dnssec-multi-signer list

An IETF draft will be developed in the near future

(based on an updated draft-johani-dnsop-multi-provider-requirements)