RFC Adjustments for Multi-Signer

IETF 113, Vienna

Shumon Huque, Ulrich Wisser
Email: shuque@gmail.com, ulrich@wisser.se

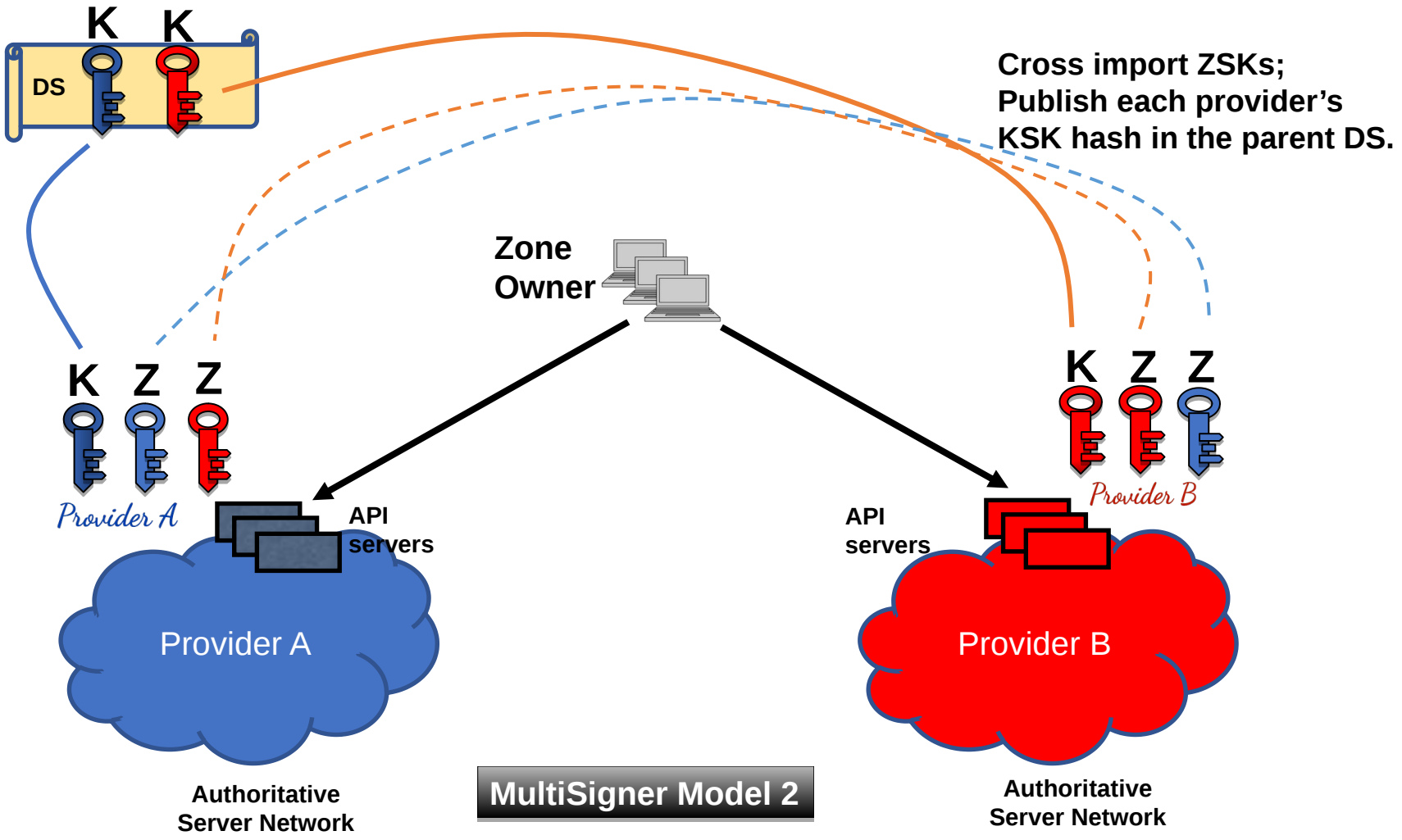
Goal

- Address some specific inconsistencies and limitations in the DNS protocol specifications (RFCs) that pose challenges for certain modes of multi-signer operation. And that are unnecessary and fixable.

Recap: RFC 8901: Multi-Signer DNSSEC

- Goal: allow multiple DNS providers to serve the same zone using their own DNSSEC signing keys.
- Introduces new key management mechanisms to make this possible.
- Two Models:
  - 1. Common KSK Set, Unique ZSK Set per Provider
  - 2. Unique KSK Set and ZSK Set per Provider

Model 2 is the most interesting, because it also offers a non-disruptive solution to inter-provider signed zone transfer. A model 2 multi-signer configuration can be viewed as a transitional state of a provider transfer.


K K
DS
Cross import ZSKs;
Publish each provider's
KSK hash in the parent DS.
Zone
Owner
K Z Z
Provider A
API
servers
Provider A
K Z Z
Provider B
API
servers
Provider B
Authoritative
Server Network
MultiSigner Model 2
Authoritative
Server Network

Challenge: Differing DNSSEC Algorithms

- If providers use different algorithms, they cannot participate in a multi-signer configuration due to restrictions imposed by the current DNSSEC protocol specifications.
- This also prevents the use of the multi-signer protocol to non-disruptively transfer a signed DNS zone to a new provider that uses different algorithm(s).
- **This is an operational gap that should be closed.**
- We expect the presence of providers supporting distinct algorithm sets to be more common over time, since there will be more algorithms (RSASHA256, RSASHA512, ECDSAP256, ECDSAP384, ED25519, ED448, PQC1, PQC2, …)

RFC 4035: Protocol Modifications for DNSSEC

Section 2.2 (last paragraph)

There MUST be an RRSIG for each RRset using at least one DNSKEY of each algorithm in the zone apex DNSKEY RRset. The apex DNSKEY RRset itself MUST be signed by each algorithm appearing in the DS RRset located at the delegating parent (if any).

This requirement cannot be satisfied if the DNS providers in a multi-signer configuration are using different signing algorithms.

RFC 6840: DNSSEC Clarifications

Section 5.11

This requirement applies to servers, not validators. Validators SHOULD accept any single valid path. They SHOULD NOT insist that all algorithms signaled in the DS RRset work, and they MUST NOT insist that all algorithms signaled in the DNSKEY RRset work.

The 2 assertions in 4035 and 6840 are (arguably) not self consistent. If validators should accept ANY single valid path, then why should signers be required to sign zone data with one of EACH algorithm in the DNSKEY set?

RFC 6840: DNSSEC Clarifications

Section 5.11

This requirement applies to servers, not validators. Validators SHOULD accept any single valid path. They **SHOULD NOT** insist that all algorithms signaled in the DS RRset work, and they MUST NOT insist that all algorithms signaled in the DNSKEY RRset work.

The use of “SHOULD NOT” here seems to be part of the problem. If this had been “MUST NOT”, then multi-signer configurations could be deployed across signers with different algorithms (implementations permitting), and we could dismiss validators that attempted to enforce such a requirement as not compliant with the specification.

Validation Reqirements

- Having all algorithms in all answers let’s validators chose
- Having only a subset of algorithms in answers requires validators to accept one algorithm or chase nameservers with answer from the other algorithms
- Or treat the domain as insecure (but signaling would be needed)

But algorithm downgrade protection?

- Requiring signing by all algorithms allows validators to detect algorithm downgrade attacks (e.g. via signature stripping).
- But this rationale is not stated anywhere in the specs.
- And in the general case, only the zone owner knows the intent of their use of multiple algorithms (e.g. for multi-signer operation, for provider transfer, or whether they desire algorithm downgrade protection).
- Validators should not unilaterally impose requirements that interfere with the zone owner’s actual intentions.
- One option would be to add additional signaling to the protocol to allow precise expression & determination of this intent.

Where could this be signaled?

- In the DS record set, but it lacks flags. So, the usual approach is a DS record “hack”: create a new “pseudo” DNSSEC algorithm number, and use a DS record entry that references that algorithm number, but carries in its data field, the required signaling information.
- In the flags of the DNSKEY record(s).
- [Your idea here]

What needs to be signaled?

- Do not enforce requirement for all data to be signed by all available algorithms in the DNSKEY set
  - either because this is a multi-signer configuration, a zone in transition across providers with disjoint algorithms, or simply because the zone owner doesn’t care about algorithm downgrade protection.
- Enforce requirement for all data to be signed by all available algorithms in the DNSKEY set.
  - e.g. because the zone owner wants to provide algorithm downgrade protection, and wants to allow validators to be able to authenticate data using all algorithms, which will include the strongest available algorithm.
- Something else (something will always come up in the future)

Write up a proposal for IETF

- We are planning to write up a specific protocol enhancement proposal for consideration by the IETF DNS Operations Working Group.
- Collaborators welcome.