Multi-Signer Protocols

ICANN 70 DNSSEC Workshop

Shumon Huque & Ulrich Wisser

March 24th 2021

Multi-Signer DNSSEC models

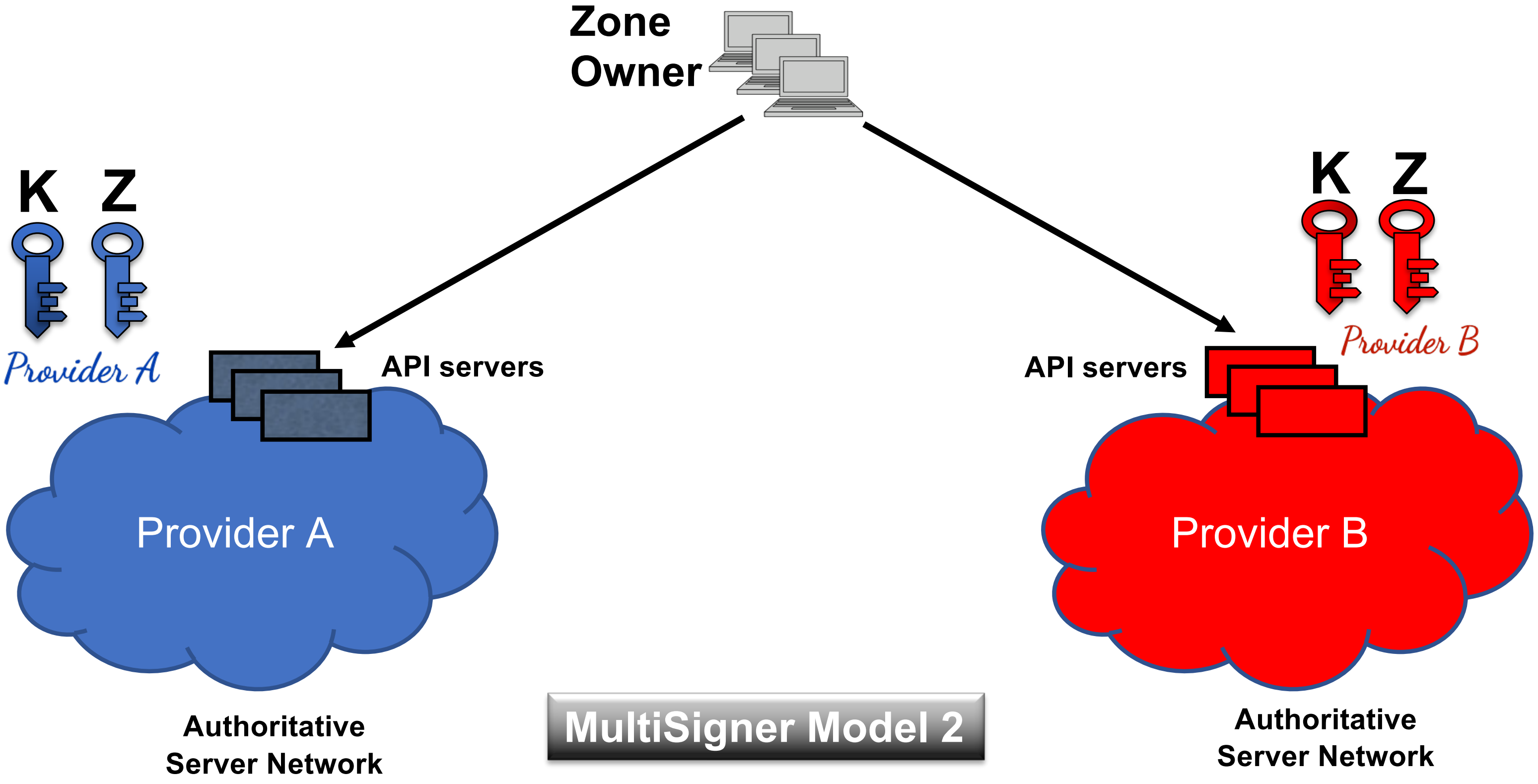
- Overview of the Multi-Signer DNSSEC protocol (RFC 8901)
  - Focus on Model-2 (Each provider has their own KSK/ZSK sets)
  - Most likely to be deployed
  - Direct relation to the topic of Operator transfer of signed zones

- New work: Bootstrapping and automating a multi-signer configuration

Multi-Signer DNSSEC models

- RFC 8901: https://www.rfc-editor.org/rfc/rfc8901.html
- Each DNS provider signs zone data with their own keys.
- Zone Signing (public) keys are shared across providers
- Zone owner uses provider specific zone management APIs to update zone content at each provider.
- We will focus on Model 2; more generally useful; and is directly related to transfer of service between operators.

Each provider has their own KSK and ZSK.



Zone Owner

K Z

Provider A

API servers

Provider A

Authoritative Server Network

K Z

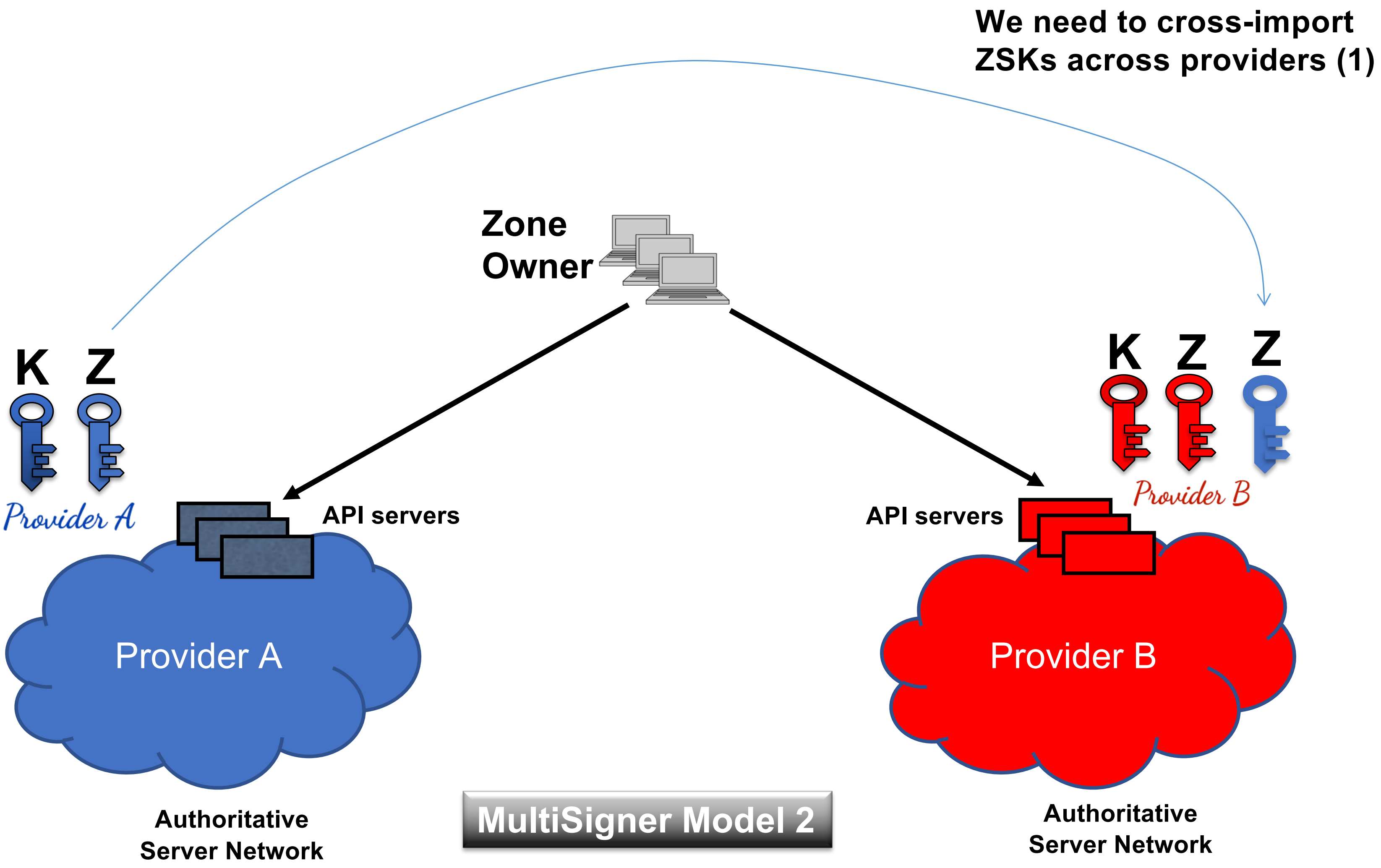
Provider B

API servers

Provider B

Authoritative Server Network

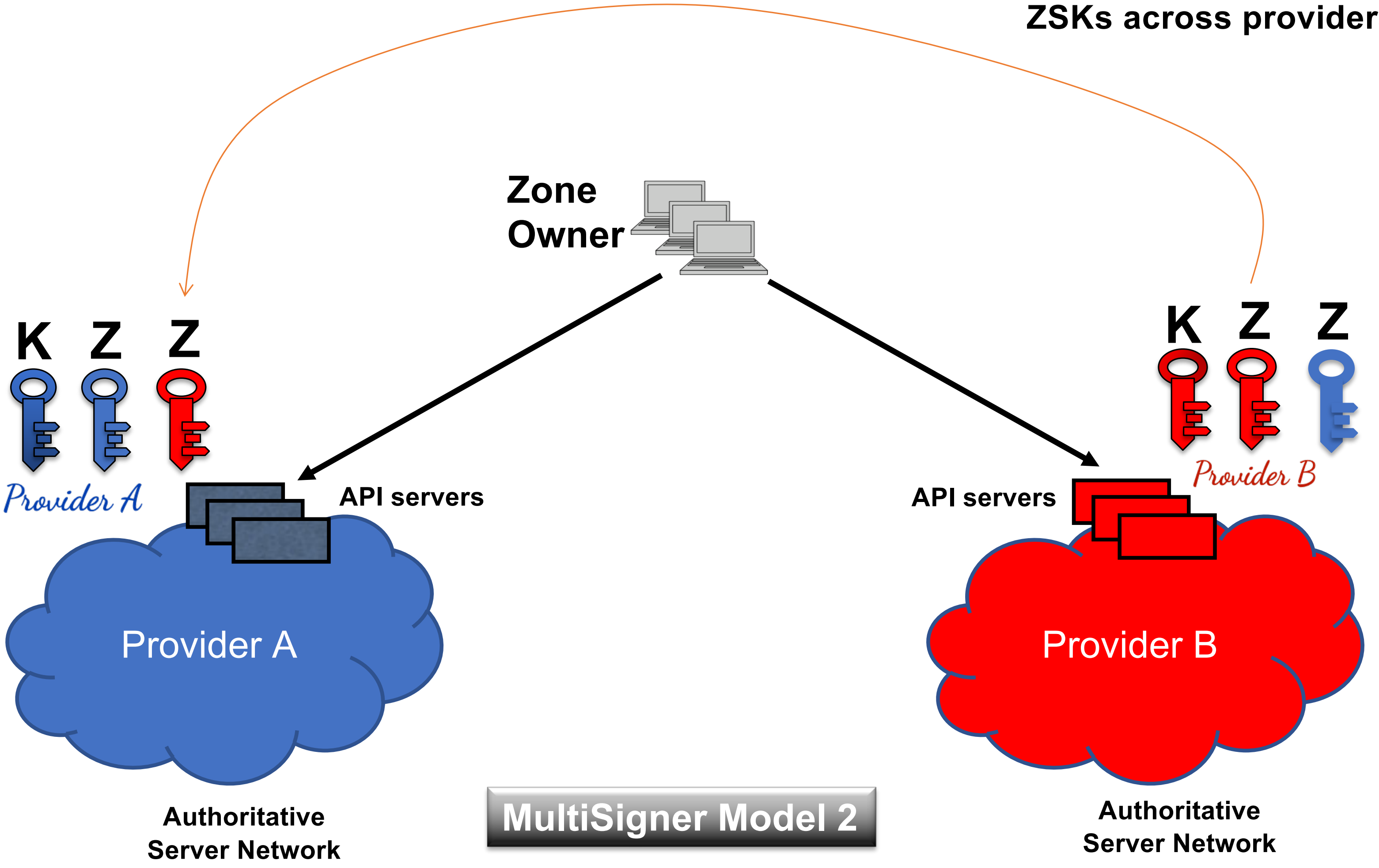
MultiSigner Model 2



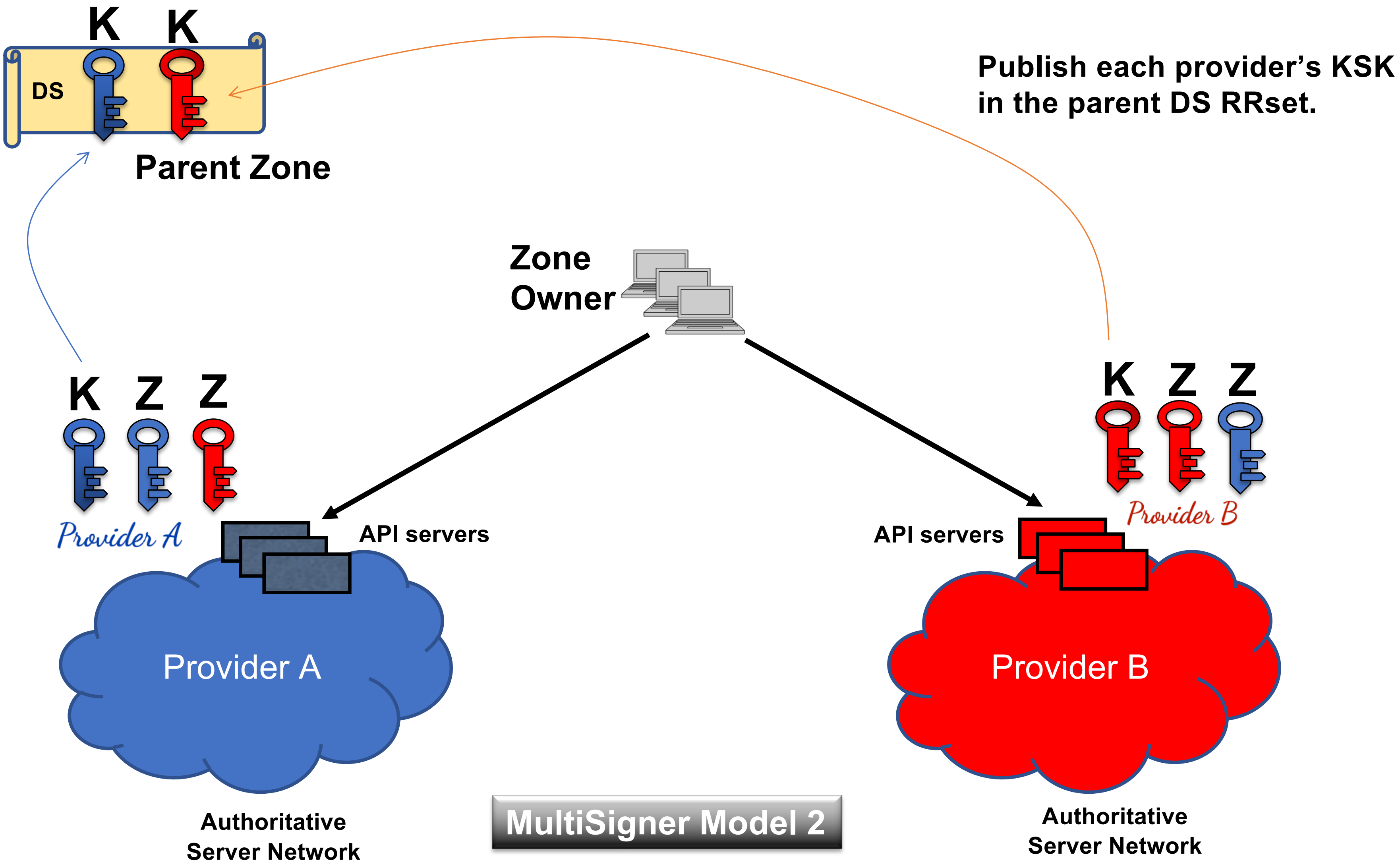
We need to cross-import ZSKs across providers (1)

MultiSigner Model 2

We need to cross-import ZSKs across providers (2)



MultiSigner Model 2



Publish each provider's KSK
in the parent DS RRset.

MultiSigner Model 2

Automating the Multi-Signer config

- RFC 8901 describes the main principles of Multi-Signer operation.
- It does not describe detailed operational procedures for initial bootstrapping of the configuration, adding additional providers, detaching providers (for operator handoff), etc.
- Or, mechanisms for automating the configuration.

Automating Multi-Signer DNSSEC

New IETF draft:

https://tools.ietf.org/html/draft-wisser-dnssec-automation-01

Initial bootstrapping of a single provider

Adding additional providers

Dropping a DNS provider to achieve non-disruptive transfer of DNSSEC signed zones

Employs CDS, CDNSKEY, CSYNC

DNS Operator hand-off

Changing the DNS operator a signed zones can be a challenge.

The most common method today is temporarily “going insecure”.

This is a bad choice for security, and a bad choice for users relying on the security of the zone.

This problem could be solved by temporarily establishing a multi-signer configuration with the new provider, and subsequently detaching the old one.

CDS, CDNSKEY records

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

These are published in the child zone (not the parent).

Child uses them to signal to the parent that the contents of the DS record in the parent should be updated.

CDS (syntactically equivalent to DS) contains the hash of the KSK(s)

CDNSKEY contains the the KSK(s)

Parent (or an intervening registrar) is expected to periodically poll them and automatically update the DS set for the child zone.

CSYNC record

RFC 7477: Child-to-Parent Synchronization in DNS

Automatically synchronize NS and glue records in parent, by periodically polling ”CSYNC” records in the child zone.

This is similar to CDS/CDNSKEY, but for the “NS set” and glue records to be automatically updated in the parent zone.

Bootstrapping a Single Provider

This process is no different from the current method of setting up a single DNS operator with DNSSEC.

- Either through registrar contract

Or

- By following RFC 8078 CDS/CDNSKEY section 3

Automating Multi-Signer DNSSEC

Two (or more) independent DNSSEC signers for the same zone

Each signer uses its own set of keys (KSK / ZSK or CSK)

Zone data synchronization is out of scope

Adding a Signer

Exchange ZSK DNSKEY RR

Wait TTL of max of all DNSKEY sets

Compute CDS/CDNSKEY RR set containing records for all KSK

Publish CDS/CDNSKEY set

Wait for parent to update

Wait TTL of DS

Remove CS/CDNSKEY set

Adding a Signer

Exchange NS sets (all signers should publish the same NS set)

Publish CSYNC record with NS and A and AAAA bit set

Wait for parent to update

Remove CSYNC record

Detaching a Provider

Zone owner signals removal intent to Multi-Signer group

Compile new NS set for remaining provider(s)

Publish CSYNC Rrset

Wait for parent to pickup changes

Remove CSYNC record from all signers

Wait 2 times TTL of maximum NS TTL from parent and all signers

Detaching a Provider

Signal all other signers leaving of multi-signer group

Stop answering queries

Remaining signers remove ZSK of leaving signer from their DNSKEY set

Calculate CDS/CDNSKEY set

All signers publish their CDS/CDNSKEY set

Wait for parent to pick up DS updates (= remove DS for detaching signer)

Remove CDS/CDNSKEY set from all signers

Automating Multi-Signer DNSSEC

TODO:

- ZSK rollover specification
- KSK rollover specification
- Algorithm rollover specification
- Specification for signers with different algorithms

Signers with Distinct Algorithms

- This cannot be supported today due to limitations in the current protocol specifications.
- It also means that we can’t non-disruptively transfer a signed zone from one operator to another operator, if they only support different algorithms.
- However it could be supported with small tweaks to the protocol.
- We are writing a protocol enhancement specification to potentially address this.
  - Relax validation rules; Introduce additional signaling.