DNSSEC & DNS MIGRATION

How to migrate your DNS without disrupting DNSSEC

Junior Payne

Contents

DNSSEC & DNS Service Provider Migration

Purpose

The purpose of this document is to propose a way to migrate DNS service providers with a DNSSEC enabled zone without turning DNSSEC off and without losing name resolution in the zone. The process described here is for situations when you have a registered domain that you, or a managed DNS service provider, manages the DNS for, and you wish to migrate your services to a new DNS service provider without impacting DNSSEC resolution for the name in the zone. A new DNS service provider is identified as the gaining DNS service provider for your zone, and the outgoing DNS service provider will be called the losing DNS service provider. In this resource, we will cover a brief description of certain DNSSEC records, the steps involved in migrating DNS service providers, and issues to be aware of in this migration process.

What we don't cover

There are other ways of migrating DNSSEC enabled DNS service provider that we don't describe for reasons of security concerns.

1. Disable DNSSEC, migrate zones, re-enable DNSSEC
2. Obtaining the private key and adding it in the gaining DNS provider

DNSSEC specific records

- CDS and CNSKEY - For a child zone requesting updates to DS record(s) in the parent zone.
- DNSKEY - Contains a public signing key.
- DS - Contains the hash of a DNSKEY record.
- NSEC and NSEC3 - For explicit denial-of-existence of a DNS record.
- RRSIG - Contains a cryptographic signature and is the signature of the zone signing key on the record set.
- ZSK – Zone Singing Key – This is the key that signs all the data in the zones.

The primary records relevant to the migration process are RRSIG, DNSKEY and DS.

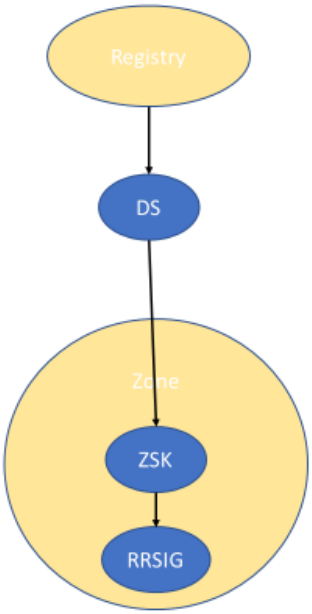
Process for transferring DNSSEC zone

1. Transfer zone to gaining DNS service provider
2. Publish the new zone – go live
3. Add gaining DNS service provider's DNSKEY ZSK to losing DNS service provider's name servers
4. Add DS record(s) of gaining DNS service provider
5. Change the delegation of the zone to the gaining DNS service provider
6. Remove DS record(s) of the losing DNS service provider
7. Remove losing DNS service provider's DNSKEY ZSK from the root zone

Detailed process

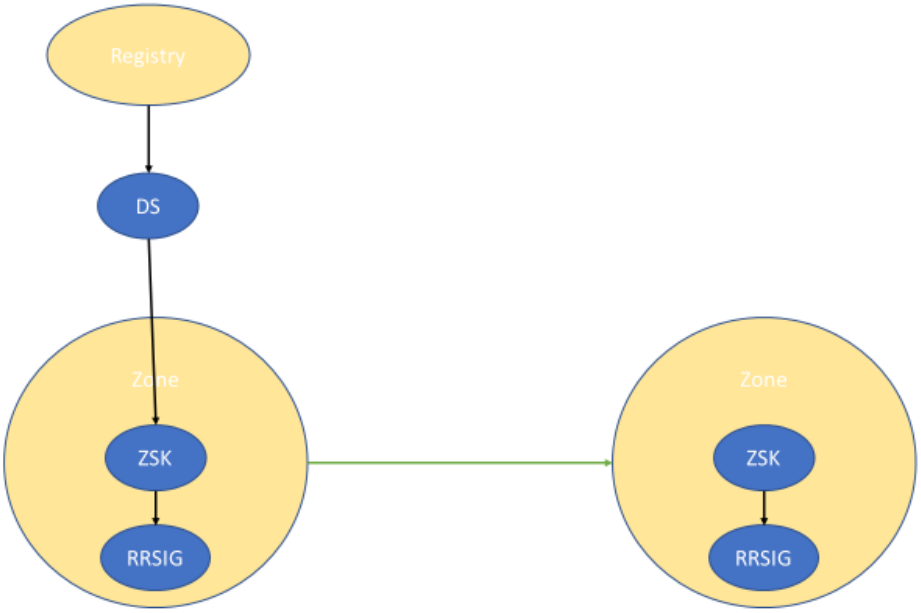
Current state

In the current state the registry has the losing DNS service provider's DS record(s) and this validates the ZSK, which then validates against the RRSIG of the record(s).



1. Transfer zone to gaining DNS service provider

Transfer the zone to the gaining DNS service provider. Usually using AXFR is the easiest way to transfer the zone. The DNSSEC keys and signatures in the zone will be transferred as well.

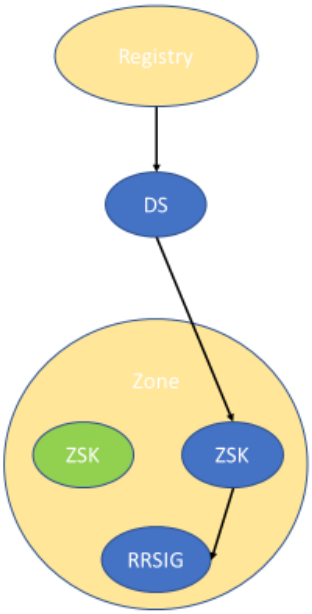


2. Publish new zone

With the gaining DNS service provider, put the newly transferred zone online in preparation of delegation.

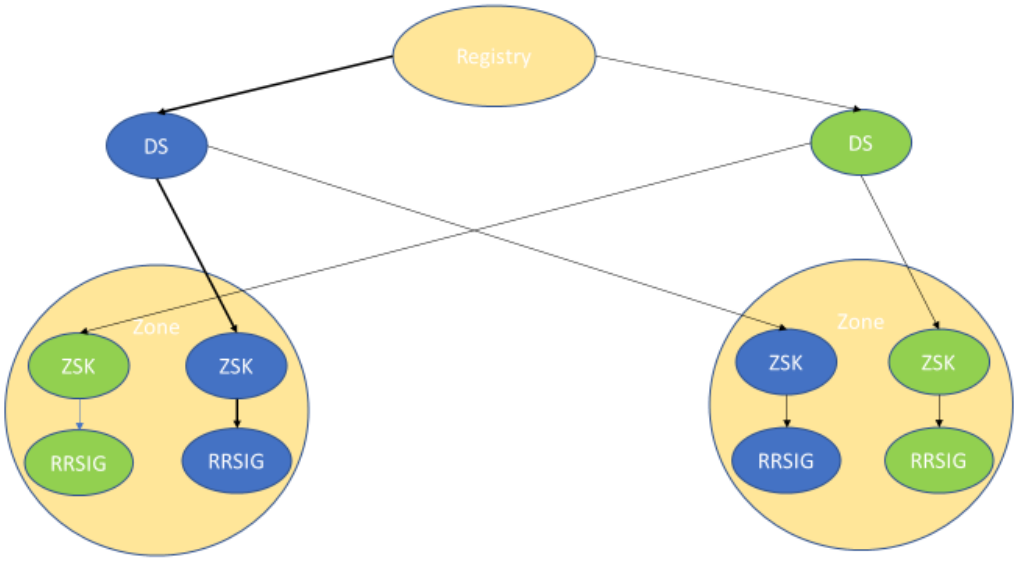
3. Add gaining DNS service provider's ZSK to losing DNS service provider

With the losing DNS service provider, add the gaining DNS service provider's ZSK. This is done in preparation of changing over the DS record(s).



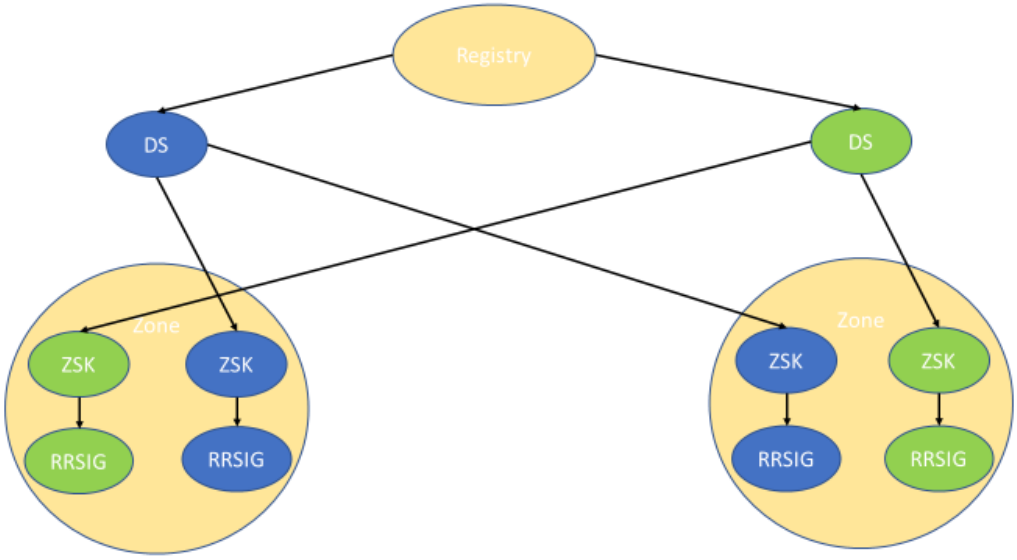
4. Add DS record(s) of gaining DNS service provider

Add the DS record(s) of the gaining DNS service provider to the registry. This current state will validate both the losing and gaining DNS service providers' ZSKs. We have not yet changed the delegation to the new name server(s).



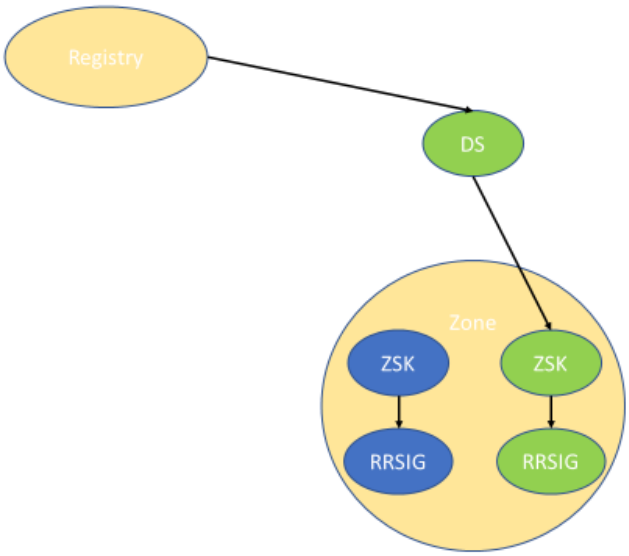
5. Change delegation of the zone to the gaining DNS service provider

Change the delegation to the gaining DNS service provider's name server(s). Once this is done, you will still have information (the DS and ZSK) in the zone that was signed by the losing DNS service provider's keys and they will continue to validate. In this configuration, you will need to re-sign the zone with the gaining DNS service provider and wait for all information to propagate through the internet (usually 24 hours, depending on the TTL that is set in the record).



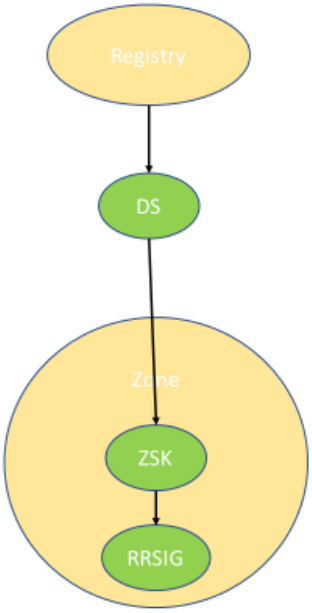
6. Remove DS record(s) of the losing DNS service provider

Once you are sure there are no longer any DS record(s) signed by the losing DNS service provider, you can remove the losing DNS service provider's DS record(s) from the registry.



7. Remove losing DNS service provider's ZSK from the root zone

The final step is to remove the losing DNS service provider's ZSK from the root zone.



Considerations

1. For simplicity, we have omitted the role of the key signing key (KSK) of the DNS operator. The KSK creates the DS record(s) and signs the ZSK. For migration purposes we are only concerned with the DS record(s) that is created by the KSK and the signature on the ZSK.
2. The losing DNS service provider's keys should remain published in the gaining DNS service provider's zone and in the registry (DS record(s)) until the largest TTL has expired.
3. In the event of an uncooperative losing DNS service provider, you do not need the private KSK from them. However, you will minimally need access to the DNS of the losing DNS service provider to publish the gaining DNS service provider's ZSK.