DNSSEC & DNS MIGRATION

How to migrate your DNS without disrupting DNSSEC

Updated: April 2019

Junior Payne
Junior.payne@geekdom.biz

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 is not covered

There are other ways of migrating DNSSEC enabled DNS service provider that are not described for reasons of security concerns, such as:

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

Definitions of DNSSEC specific records

CDS and CDNSKEY - 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.

Process for migrating a DNSSEC zone

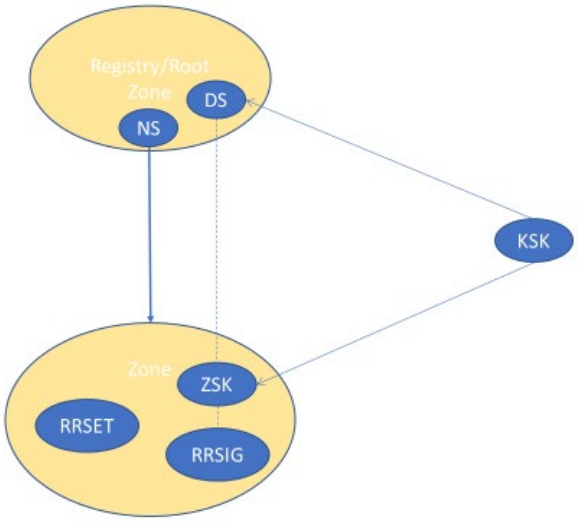
The losing provider and gaining provider must use the same DNSSEC algorithm. The primary records relevant to the migration process are RRSIG, DNSKEY and DS.

1. Copy zone to gaining DNS service provider.
2. Sign zone in gaining DNS service provider using the same algorithm as the current DNSKEY in the losing provider.
3. Publish the new zone – go live.
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.

Detailed process

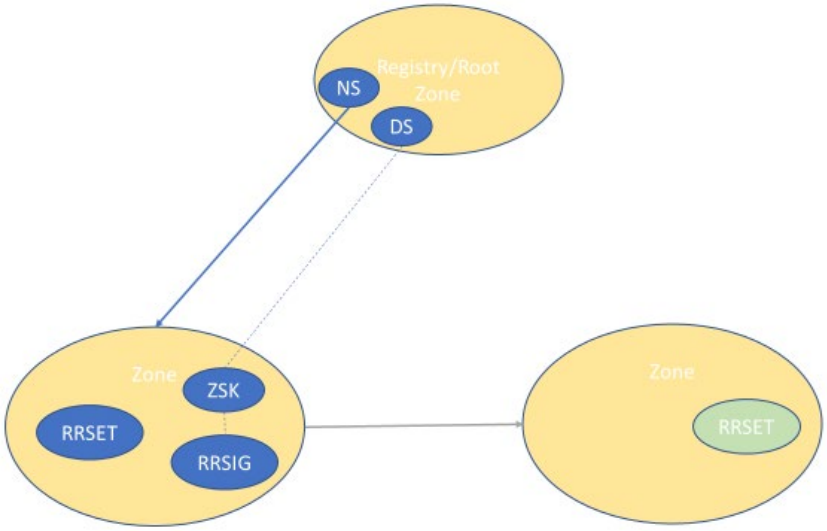
Current state

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. Copy zone to gaining DNS service provider

Copy the zone to the gaining DNS service provider. Usually using AXFR is the easiest way to copy the zone.



2. Sign the zone

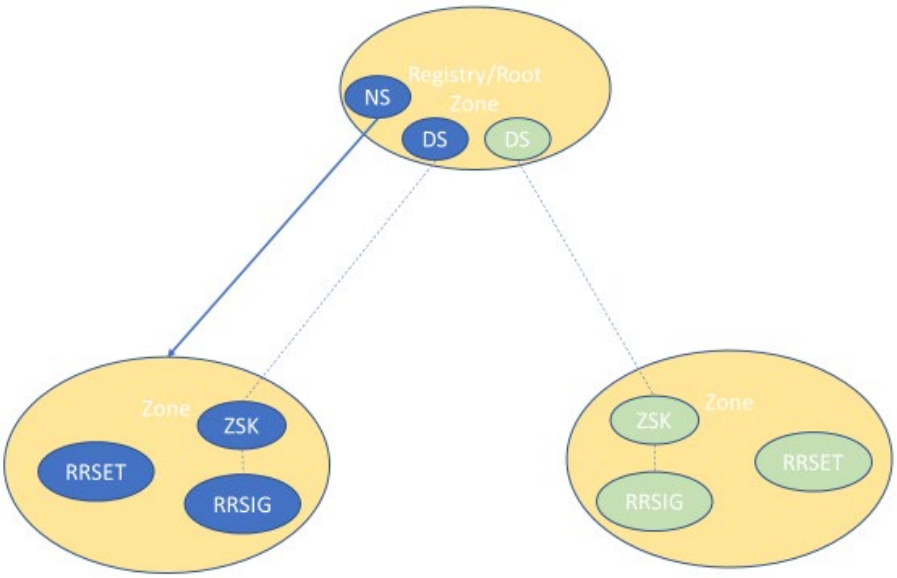
With the gaining DNS service provider, sign the zone with DNSSEC.

3. Publish new zone

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

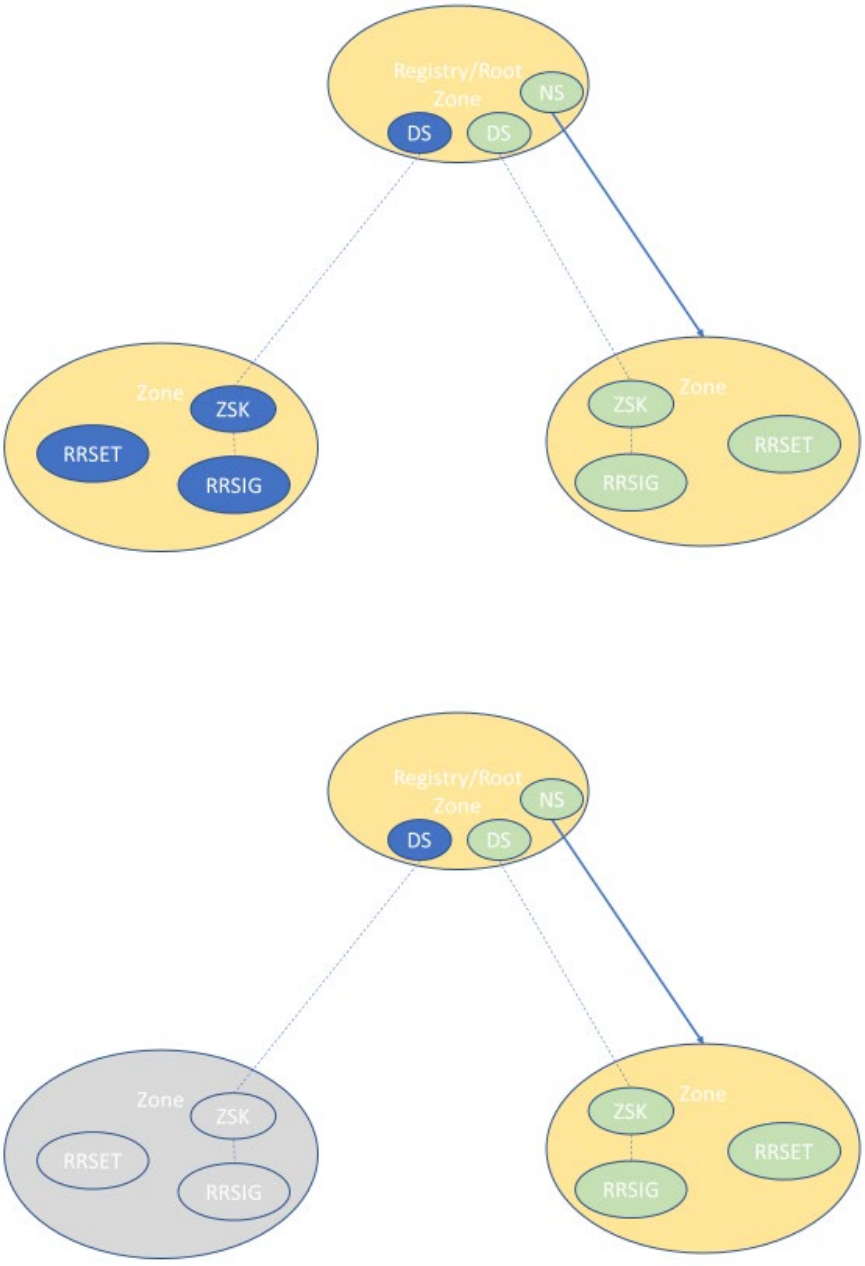
4. Add DS record(s) of gaining DNS service provider

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. At this point the delegation to the new name server(s) has not yet changed. In this configuration, it's necessary to re-sign the zone with the gaining DNS service provider and wait for all information to propagate across the internet (usually 24 hours, depending on the TTL that is set in the record).



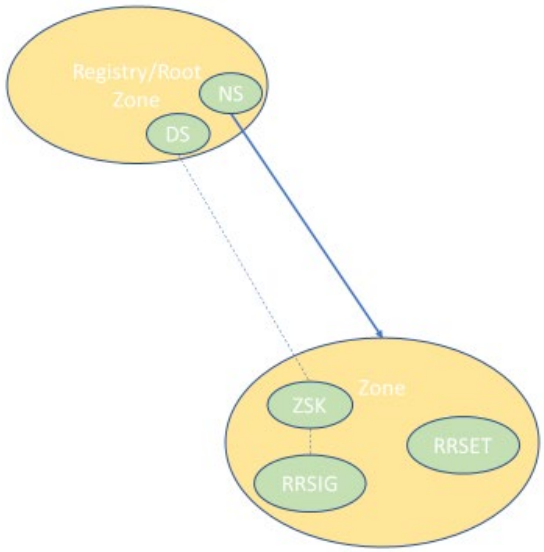
5. Change delegation of the zone to the gaining DNS service provider

Delegation is the term used to indicate what name servers have the authority to answer queries for the zone. Change the delegation by changing the name servers to the gaining DNS service provider. Once this is done, there will be 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.



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

Once you are sure there are no longer any cached DS record(s) referring to the losing DNS service provider, the losing DNS service provider's DS record(s) can be removed from the registry.



Considerations

For simplicity the role of the key signing key (KSK) of the DNS operator has been omitted. The KSK creates the DS record(s) and signs the ZSK. For migration purposes the only concern is the DS record(s) that is created by the KSK and the signature on the ZSK.

The losing DNS service provider's zone should remain published until the largest TTL has expired for the losing provider's DS record in the registry (DS record(s)).