fTLD
Registry Services, LLC

How to Avoid Disruption During DNSSEC & DNS Vendor Migration

Contents

DNSSEC & DNS Vendor Migration

Purpose

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

What is not covered

There are other ways of migrating DNSSEC enabled DNS vendor 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 system.

Disabling DNSSEC, as in item 1, would result in loss of name resolution in the zone, so that is not recommended and therefore not covered.

Definitions of 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 or DS Key - Contains the hash of a DNSKEY record. Also known as the DS 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 Signing Key – This is the key that signs all the data in the zones.

Process for migrating a DNSSEC zone

The losing and gaining vendors should use the same DNSSEC algorithm; for purposes of simplicity this document keeps the algorithms the same, but in practice you can use mixed algorithms.[1] The primary records relevant to the migration process are RRSIG, DNSKEY and DS.

1. Copy zone to gaining DNS vendor.

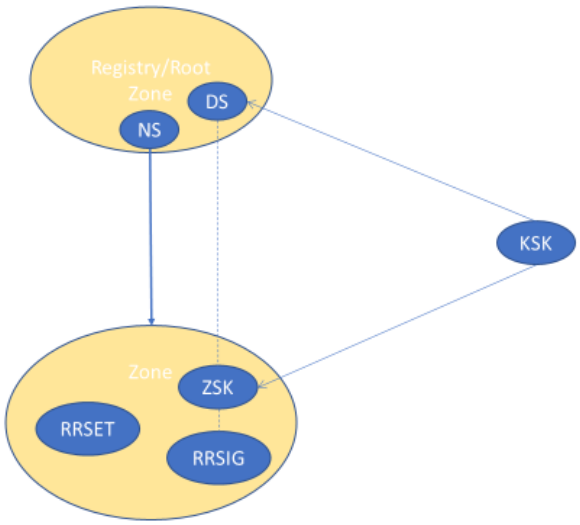
[1] To ensure there is no down time, the new published zone that is signed must match the new DS Key and the old potentially cached zone still has a DS Key in the registry. Then, once the results are no longer being cached (i.e., the TTL has expired) you can remove the old DS Key.

2. Sign zone in gaining DNS vendor 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 vendor.
5. Change the delegation of the zone to the gaining DNS vendor.
6. Remove DS record(s) of the losing DNS vendor.

Detailed process

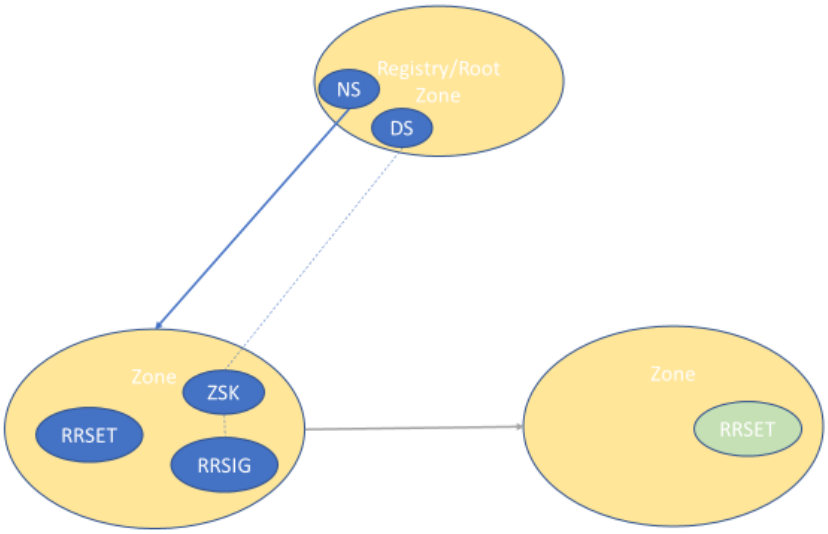
Current state

In the current state the registry has the losing DNS vendor'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 vendor

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



2. Sign the zone

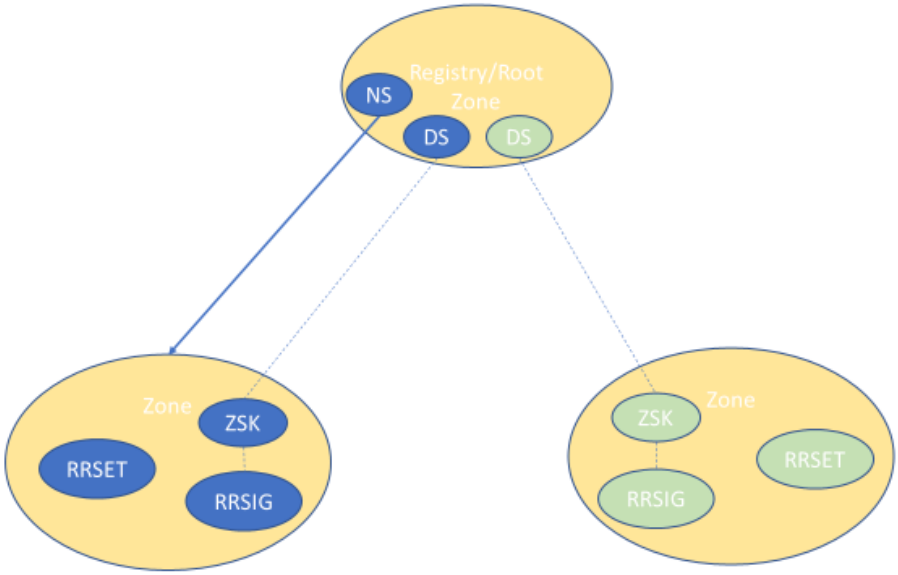
With the gaining DNS vendor, sign the zone with DNSSEC.

3. Publish new zone

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

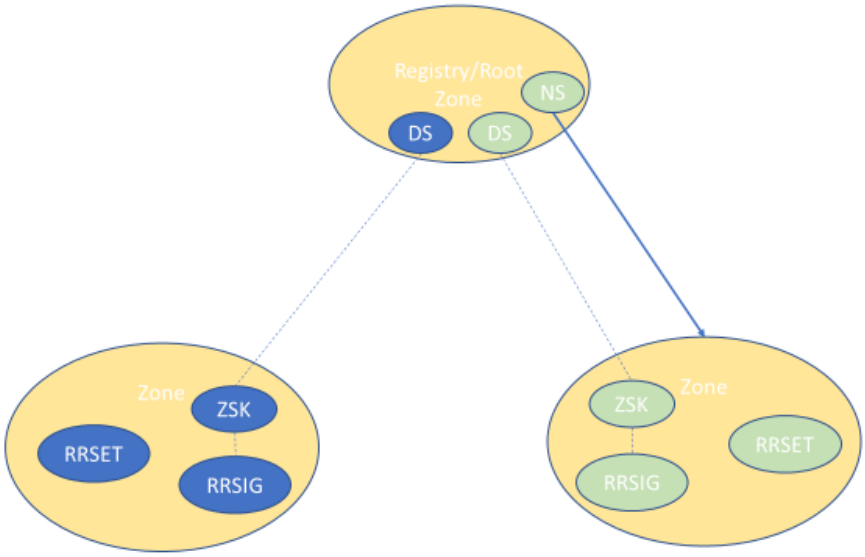
4. Add DS record(s) of gaining DNS vendor

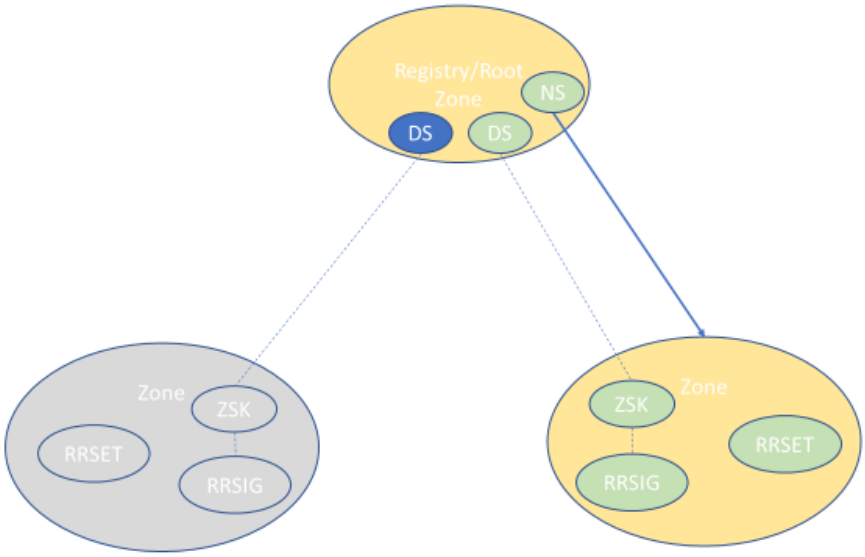
Add the DS record(s) of the gaining DNS vendor to the registry. This current state will validate both the losing and gaining DNS vendors' ZSKs. At this point the delegation to the new name server(s) has not yet changed. In this configuration, it's necessary to re-sign the zone with the gaining DNS vendor and wait for all information to propagate across the internet (usually 24 hours, depending on the TTL that is set in the record).


Registry/Root
Zone
NS
DS
DS
Zone
ZSK
RRSET
RRSIG
Zone
ZSK
RRSET
RRSIG

5. Change delegation of the zone to the gaining DNS vendor

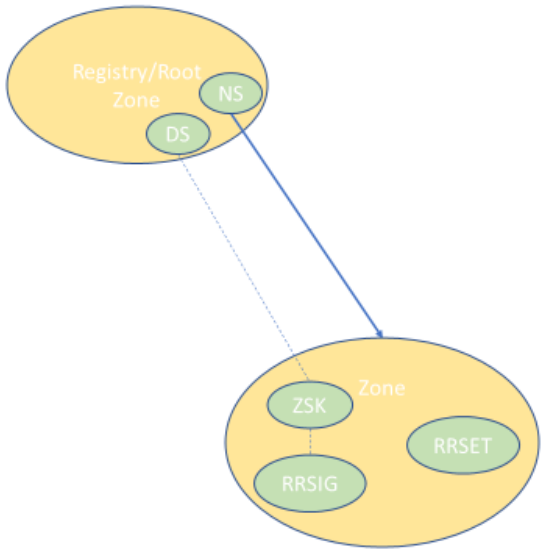
Delegation is the term used to indicate what name servers have the authority to answer queries for the zone. Change the delegation by changing the name servers to the gaining DNS vendor. Once this is done, there will be information (the DS and ZSK) in the zone that was signed by the losing DNS vendor's keys and they will continue to validate.





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

Once you are sure there are no longer any cached DS record(s) referring to the losing DNS vendor, the losing DNS vendor'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. There appears to be general consensus that the KSK should be rolled over once per year, and ZSK roll over frequency ranges from between 90 days to 12 months; auditing the ZSK key for misuse is difficult and protecting it long-term is difficult since it is constantly used so changing to more frequently than the KSK is recommended.