



---

# A Resilient DNSSEC Implementation

June 2017, ICANN-59, Johannesburg

**David Peall**  
david@dns.business

## Who is DNS Business

- Backend Registry Service Provider (RSP).
- Provide innovative RSP services for ccTLD's, geoTLD's, gTLD's and Brands.
- Dynamic registry software developed in-house. Customised policies to the Registry Operators requirements.

## Phase 1 – Redundant Signers

- Database replication for key management in the signing software.
- File system replication for key data for the HSM key store.
- Multiple HSM's configured with the same master key.

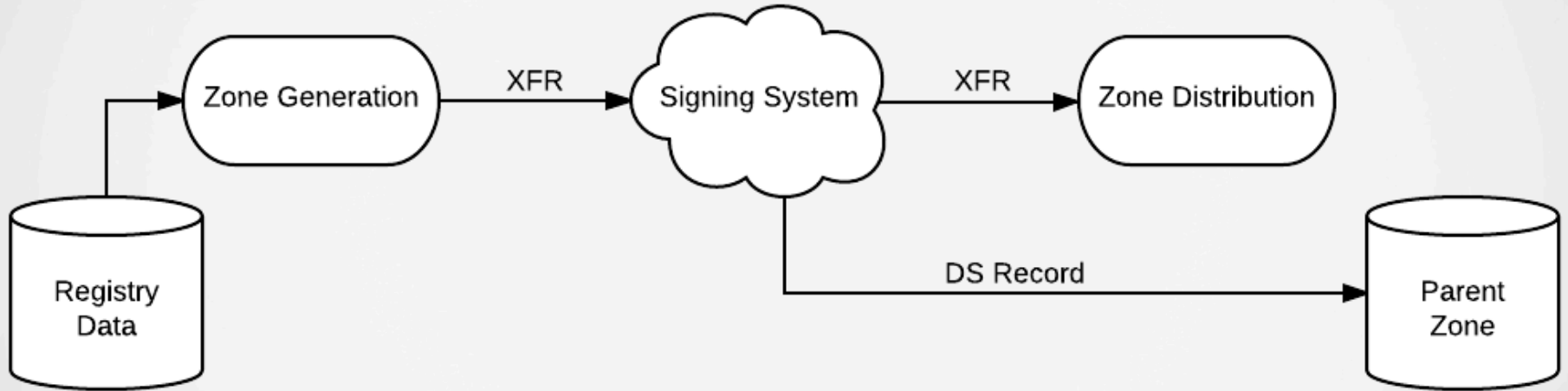
## Phase 1 – Concerns

- Replication does not prevent corruption of the data.
  - Regular database backups.
  - Regular file system backups.
- Standby signer is dormant until required and hard to test in a live environment.
- HSM vendor lock-in.
- Signing software vendor and version lock-in.

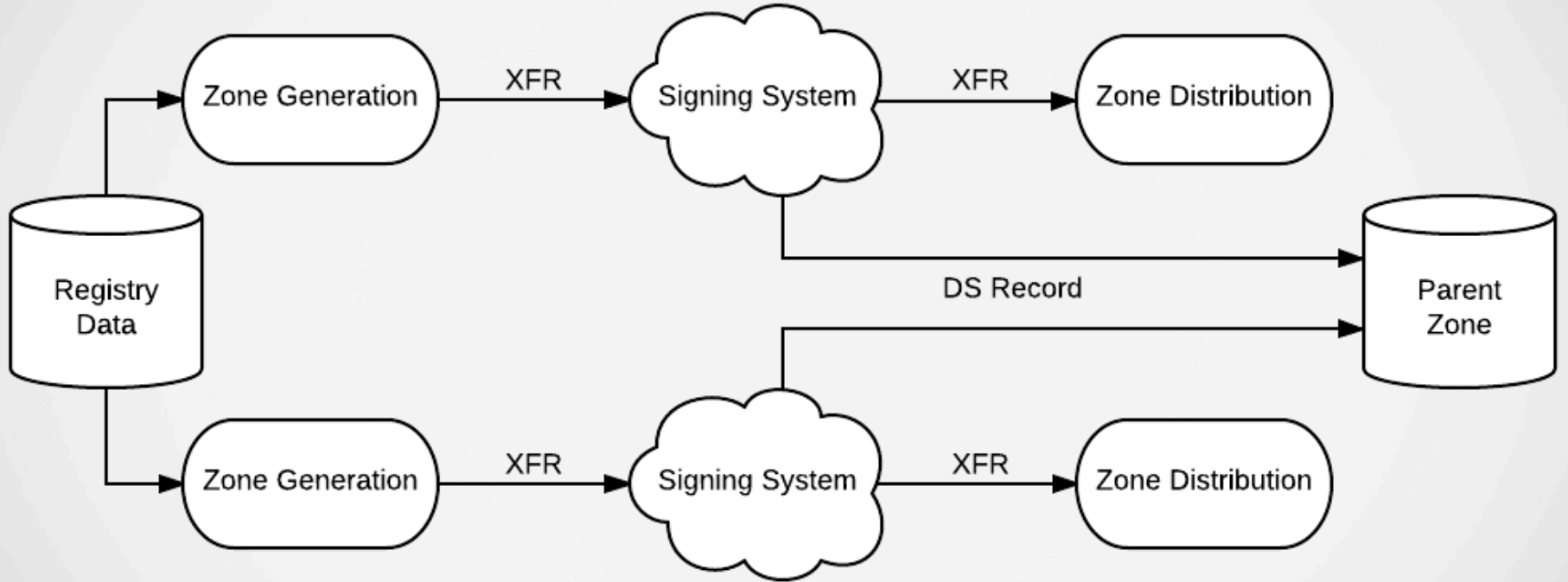
## Phase 2 – Independent Signers

- Two independently operated signing systems, these can be of the same or different software, HSM hardware and or versions.
- DS records for both systems are maintained in the parent as you would with a single signer.
- DNSKEYs (KSK,ZSK) from both signing systems are copied to the zone template where the zone is generated.
- The result is two signed zones, these zones however are interchangeable. Either zone could be published and will validate correctly due to the cross-linked DNSKEY's.

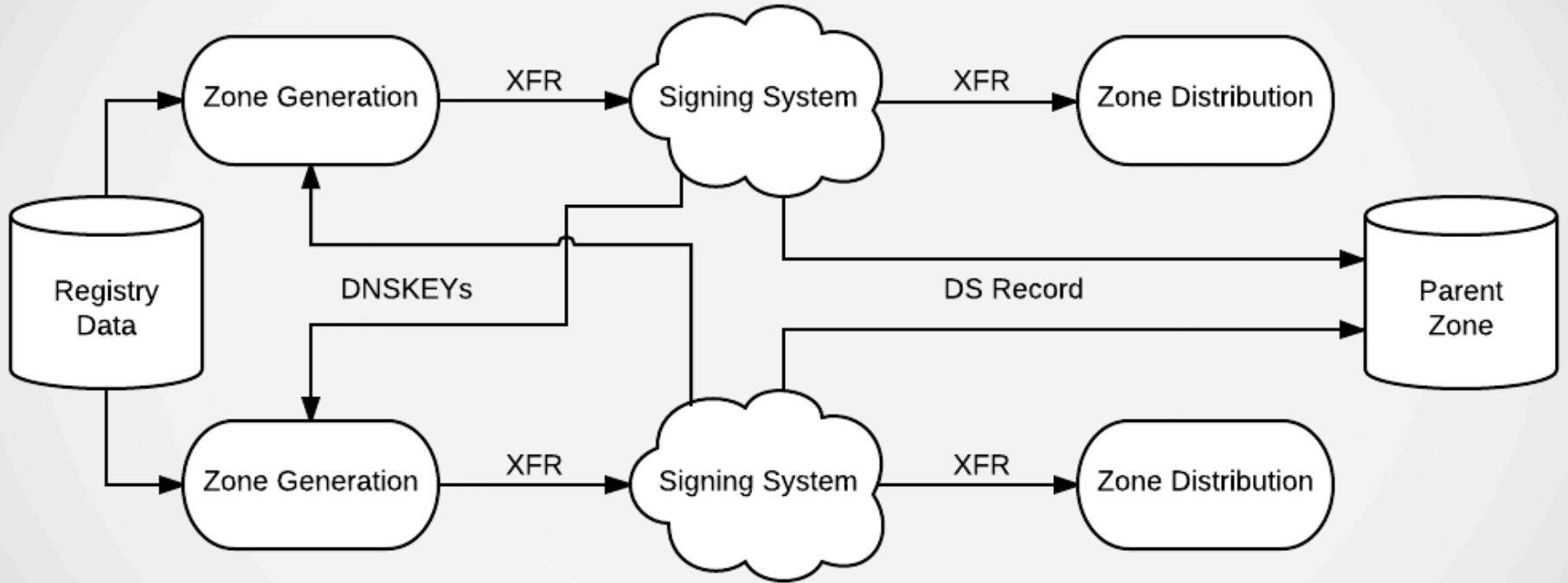
## Phase 2 – Independent Signers



## Phase 2 – Independent Signers



## Phase 2 – Independent Signers





**Questions ?**



---

## DNSSEC signed TLD - RSP Migration

June 2017, ICANN-59, Johannesburg

**David Peall**  
david@dns.business

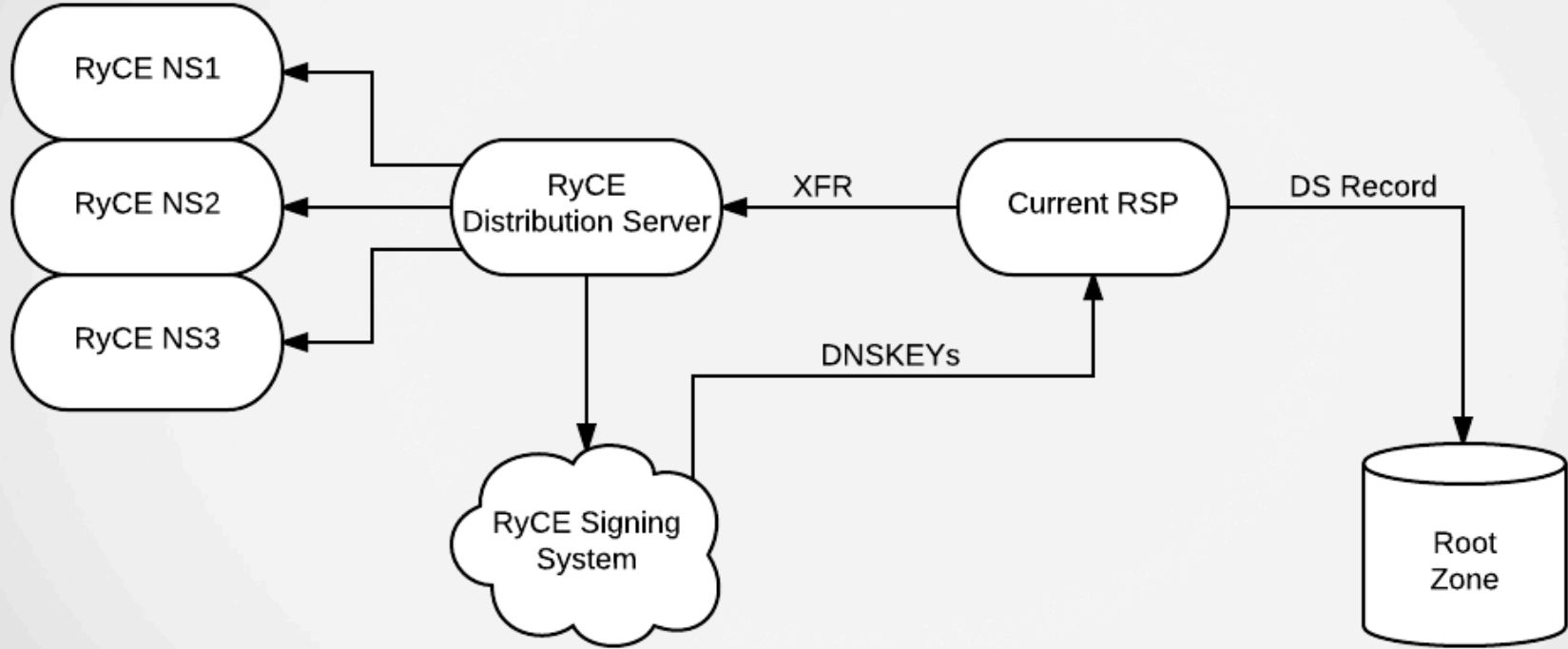
## Migrating between registry service providers

- EPP and Whois or RDDS are allowed a certain amount of downtime for the migration.
- DNS and DNSSEC need to be maintained during migration with no interruptions.

## DNSSEC Migration steps

- 21 March: Generate KSK and ZSK for the zone .wien
- 22 March: Provide the KSK and ZSK to the current RSP to be included in the zone.
- 27 March: Confirm KSK and ZSK visibility
- 27 March: IANA update – Add the new KSK's DS record in the Root Zone Management portal (RZM)
- 29 March: Slave the .wien zone from the current RSP to the new nameservers

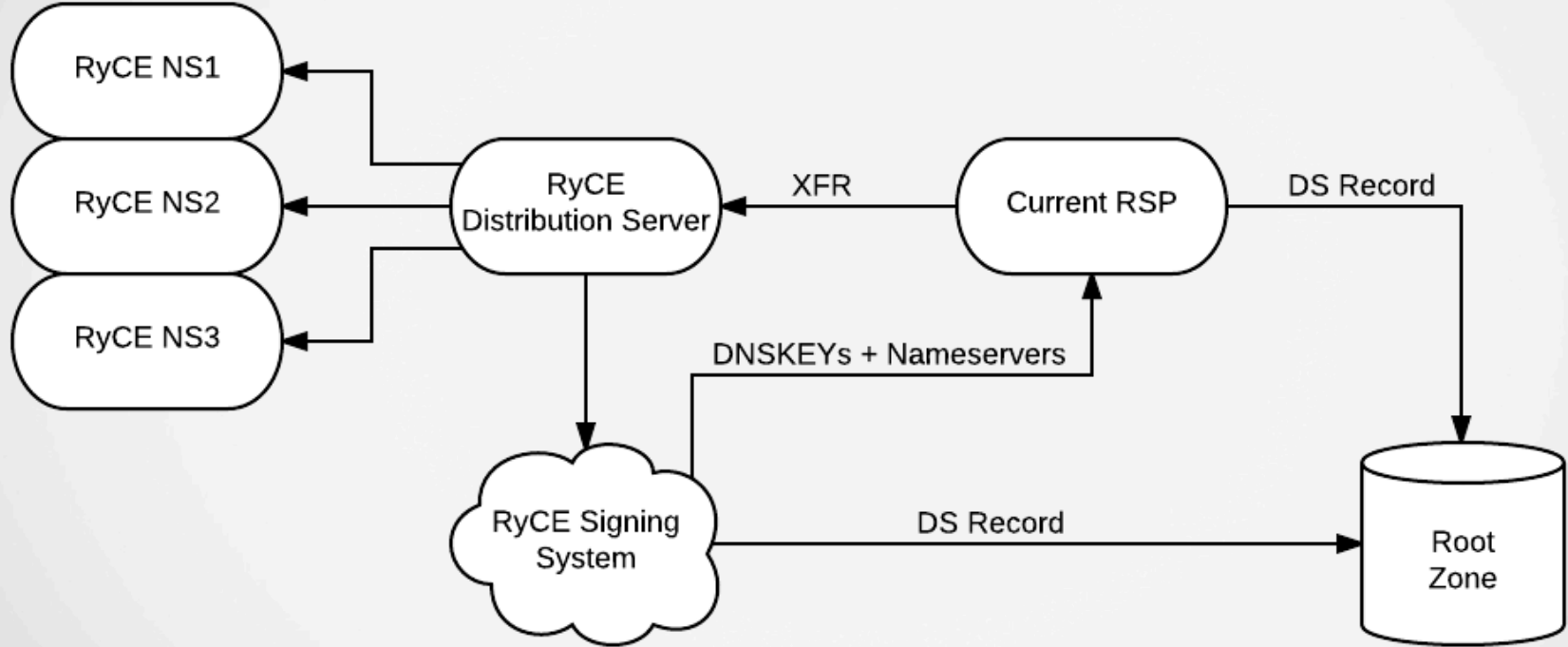
## DNSSEC Migration steps



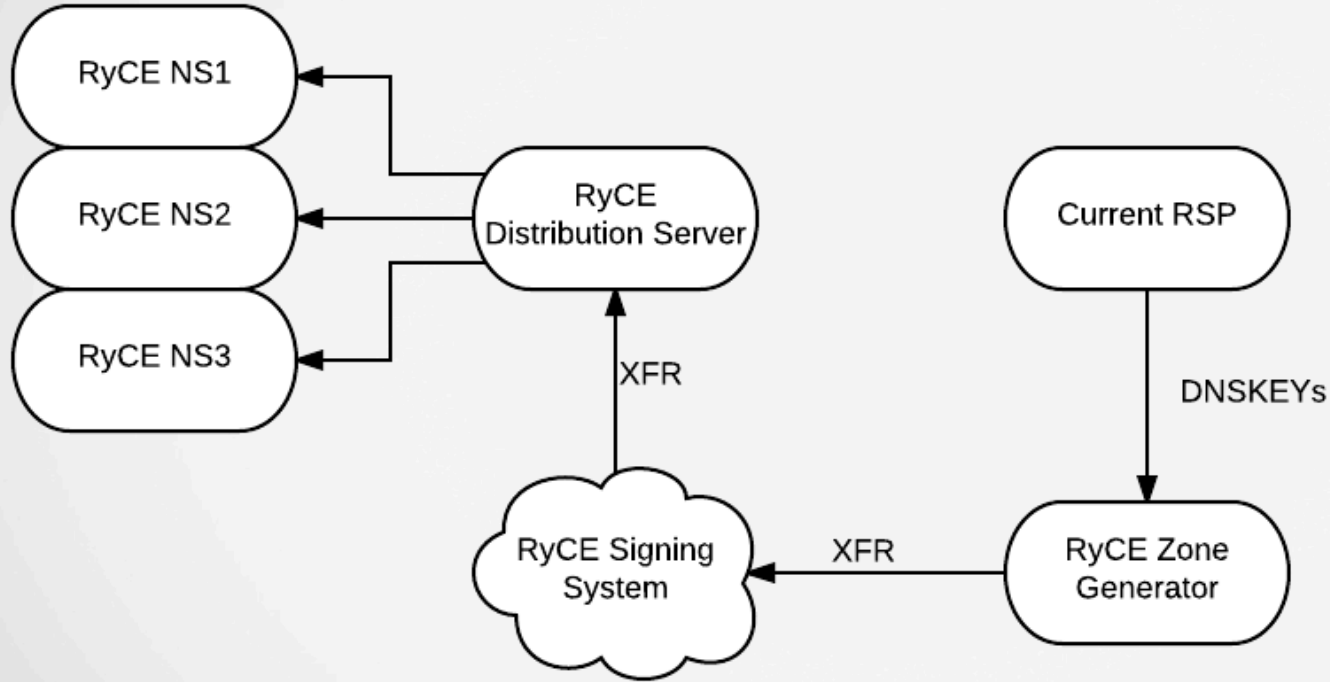
## DNSSEC Migration steps

- 29 March: Current RSP includes the new nameservers in the zone.
- 31 March: Confirm DS seen in the root from IANA update on the 27<sup>th</sup>.
- 3 April: IANA update - Add new nameservers in the RZM.
- 7 April: Confirm nameserver update from the 3<sup>rd</sup>.
- 10 April: Remove current RSP's nameservers from the .wien zone. IANA update – Remove the current RSP's nameservers.
- 14 April Confirm nameserver update from the 10<sup>th</sup>.

## DNSSEC Migration steps



## DNSSEC Migration day 24<sup>th</sup> April





**More Questions?**

Get in Touch

[www.DNS.business](http://www.DNS.business)



+27 11 568 2800



[info@dns.business](mailto:info@dns.business)



[@dns\\_za](https://twitter.com/dns_za)