

# One Aspect Of DNSSEC Automation

Žarko Kević  
 **RNIDS**

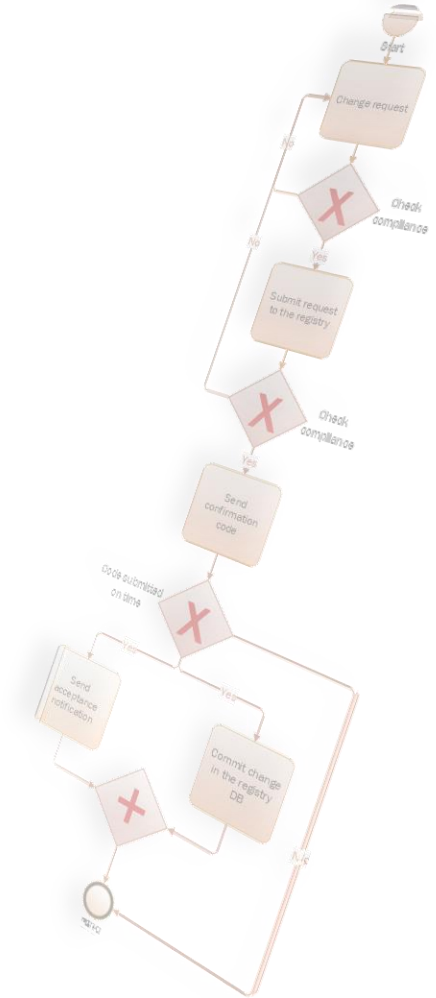
85apTLD

Goa, 19 – 22 February 2024



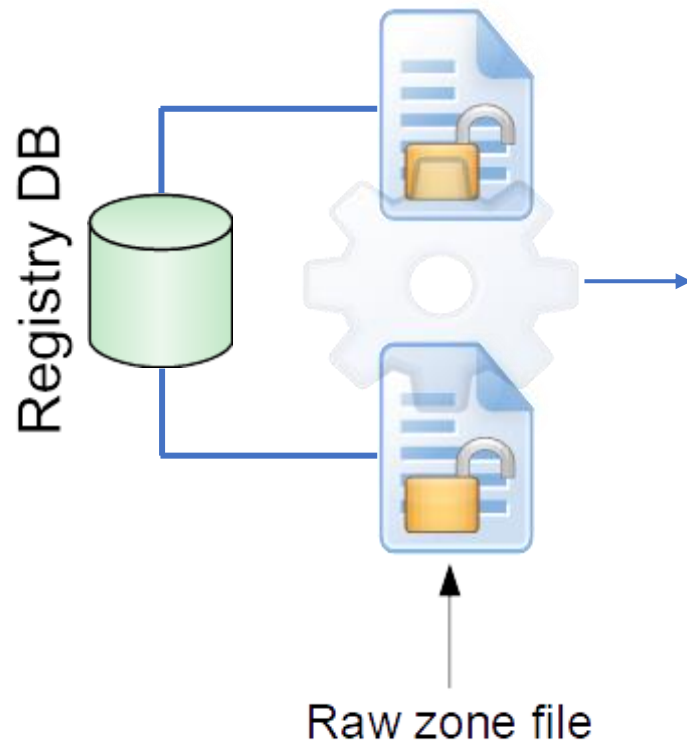
# Registry DNSSEC Signing Steps

- Unsigned zone creation
- DNSSEC signing
- Publishing of the signed zone

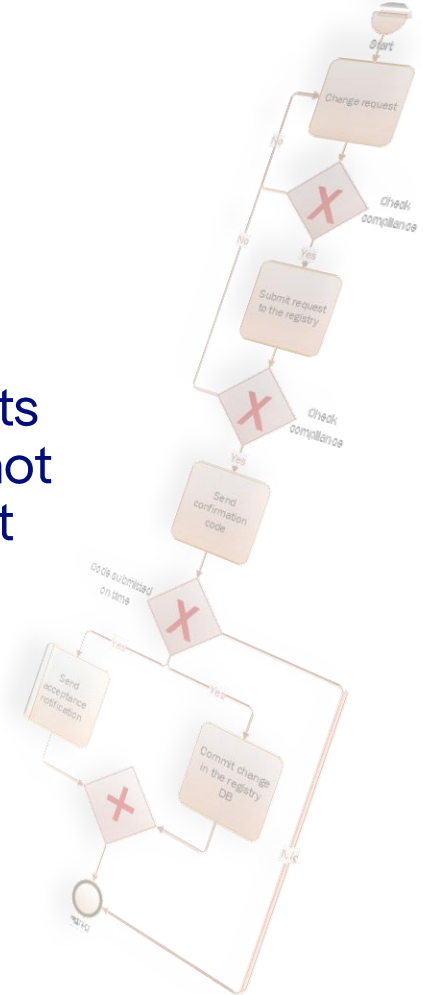




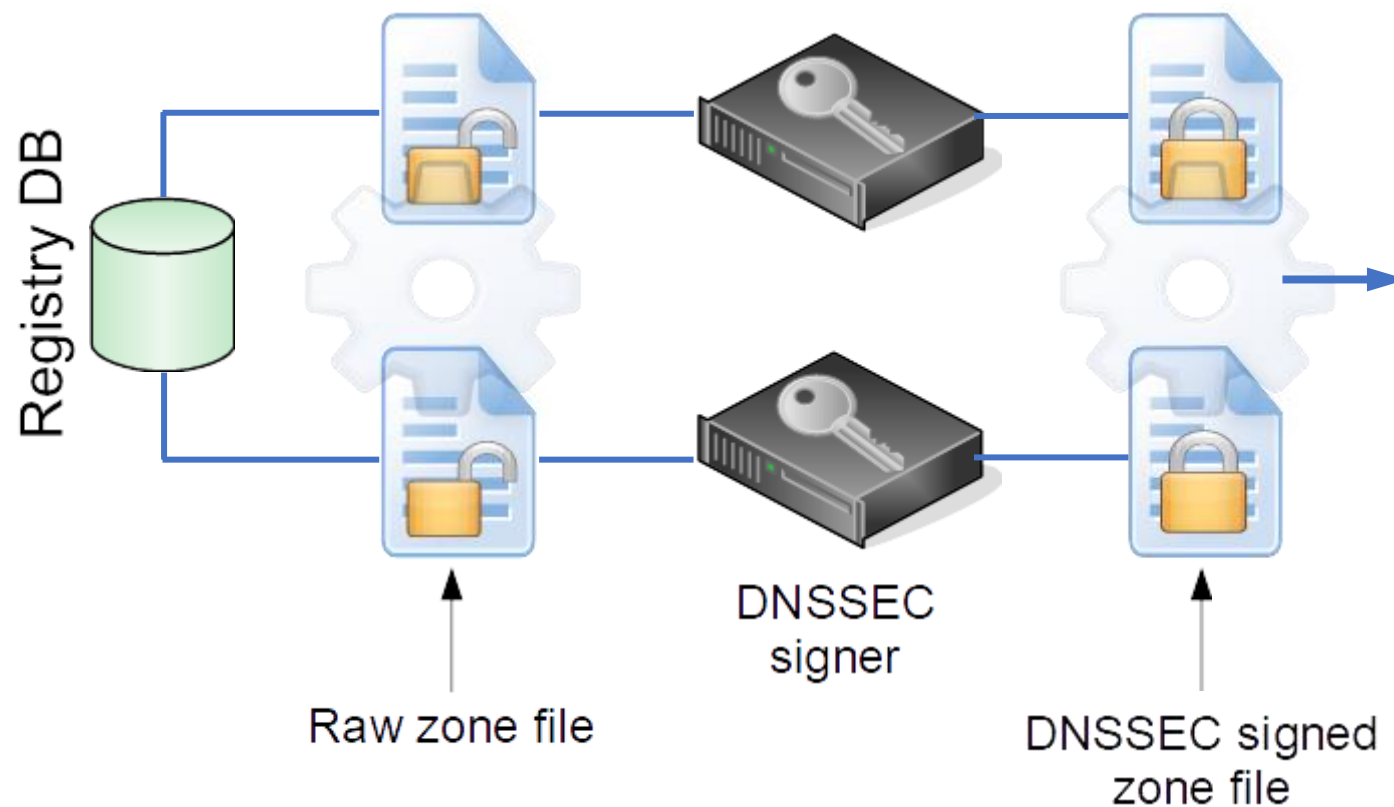
# Zone file creation



**Zone file check** - Using applications or scripts based on tools such as BIND, PowerDNS, Knot DNS, or others for zone file validation against RFC-1034, RFC-1035, and newer standards.

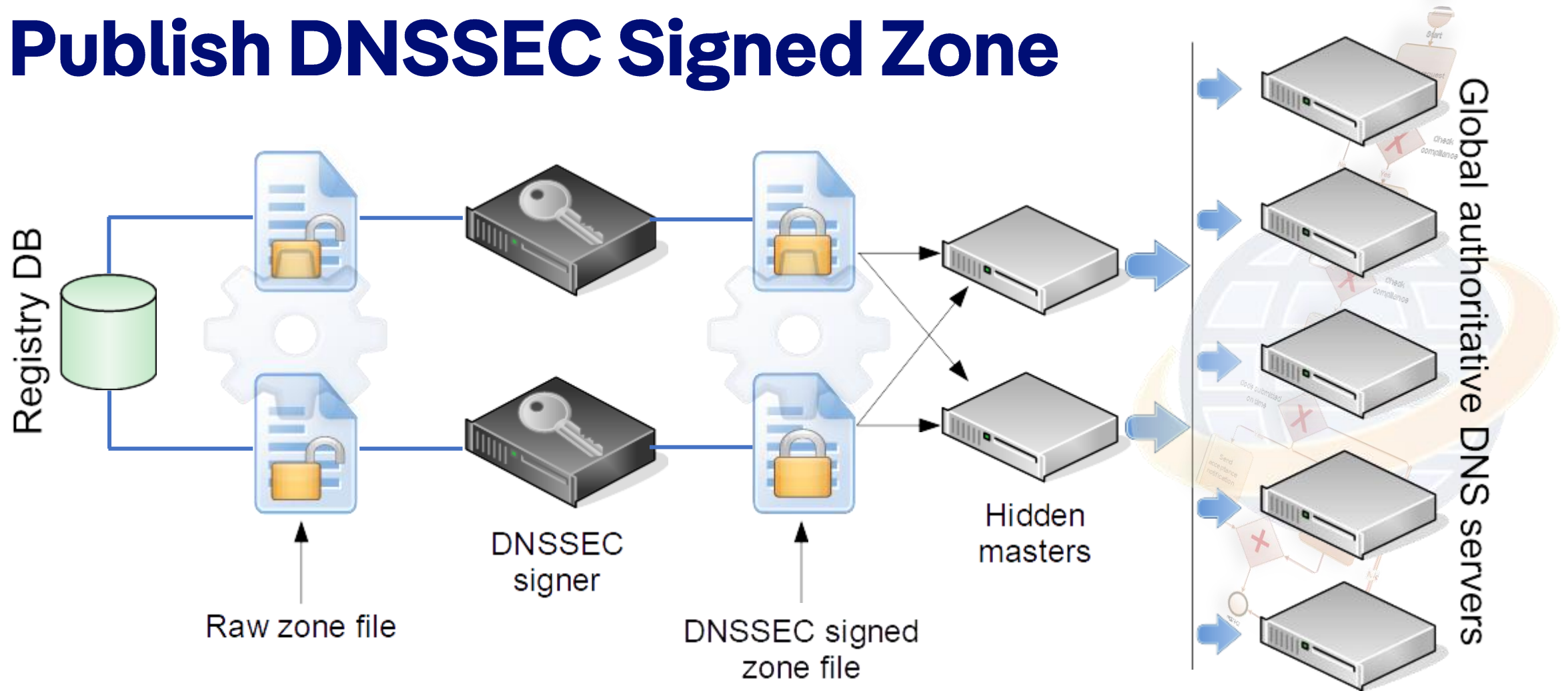


# DNSSEC signing



- **Zone file check** – e.g. ldns-verifzone reads the DNSKEY at the apex and checks the RRSIG records in the zone file against that key.
- Load the zone file as local and use DNSSEC validation tool to check signature against actual DS record.

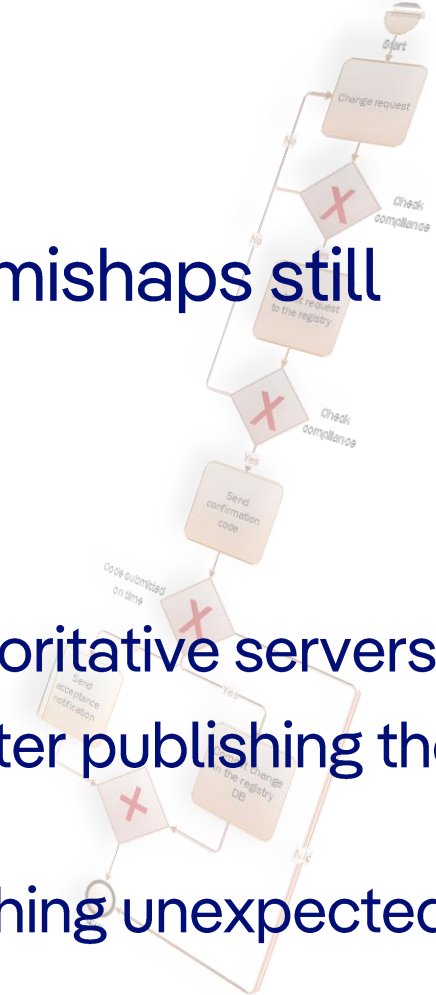
# Publish DNSSEC Signed Zone



# Resilient DNSSEC Automation

DNSSEC automation is at a higher level these days, but mishaps still occur!

- Be sure you are signing the correct zone file.
- Inspect the signed zone again for errors.
- Verify DNSSEC validation before dispatching the zone to authoritative servers.
- Perform DNSSEC validation across all authoritative servers after publishing the zone.
- Make sure to be ready to take immediate action in case something unexpected happens!



# Thank you!

