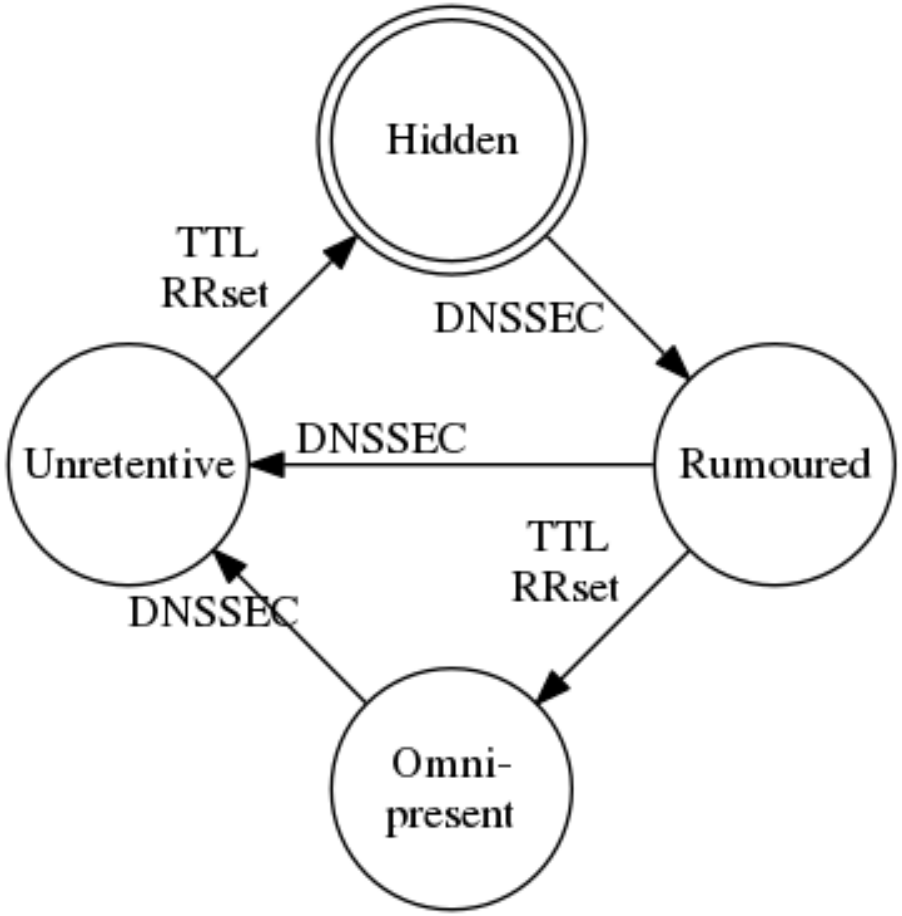
DNSSEC Operations

Timers of Various Kinds

Key-Related Timers

- We have already seen timers in action during the ZSK rollover lab
  - New timers were specified on existing keys
  - New keys were generated as successors to existing keys, ensuring that the timers associated with them made sense
- Why are timers necessary?
  - DNS is loosely-coherent
  - Responses are cached
  - Signatures have validity periods

Key States (OpenDNSSEC 2.x)



Hidden. The associated resource records are never published or are unpublised long enough that the enforcer knows no validator will try to use this resource record for validation.

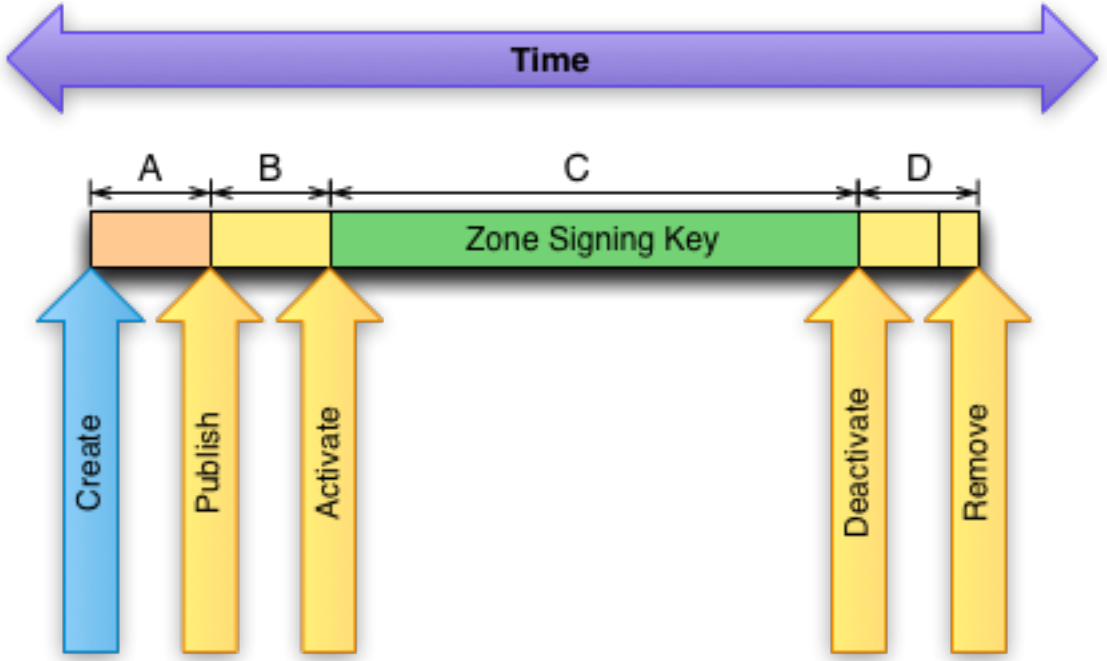
Rumoured. This record is being published but might not be accessible for all validators yet. After some time (including the TTL of record set) the state will move to omnipresent.

Omnipresent. The record is fully published and available for everyone. No caches contain any old key with an unexpired TTL.

Unretentive. The signer is instructed no longer to publish this record but it might exist in some caches still. After some time the state will move to hidden.

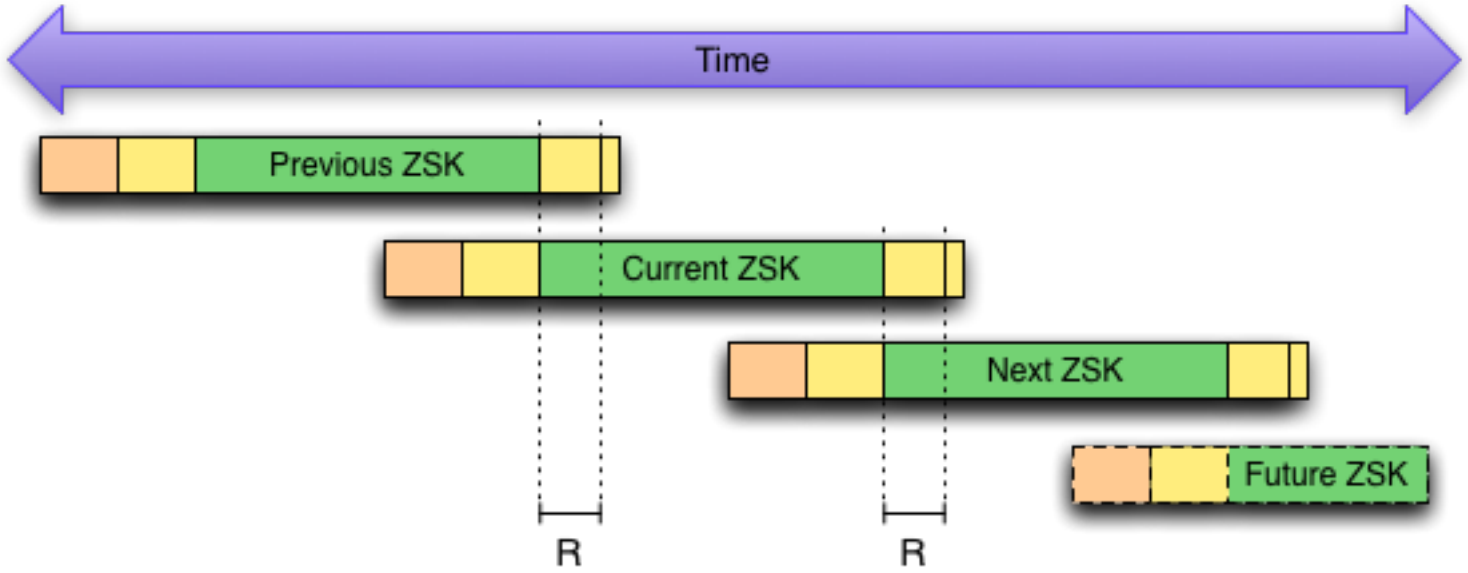
https://wiki.opendnssec.org/display/DOCS20/Key+States+Explained

Lifecycle of a key (BIND9)



https://kb.isc.org/docs/aa-00822

Lifecycle of a key (BIND9)

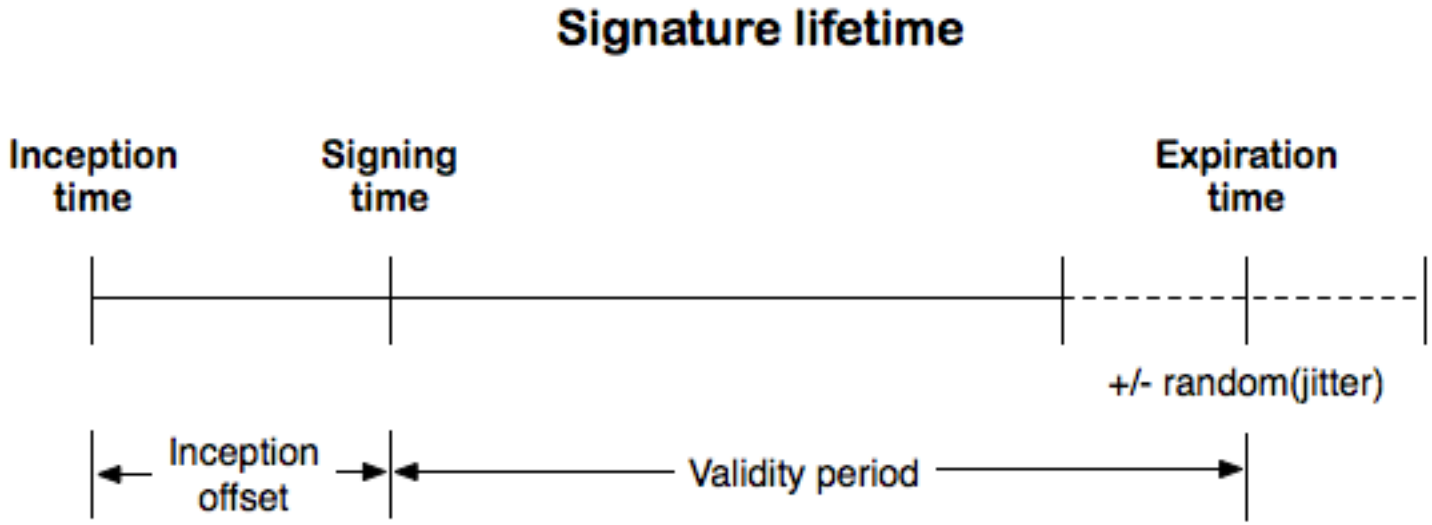


https://kb.isc.org/docs/aa-00822

Signature-Related Timers

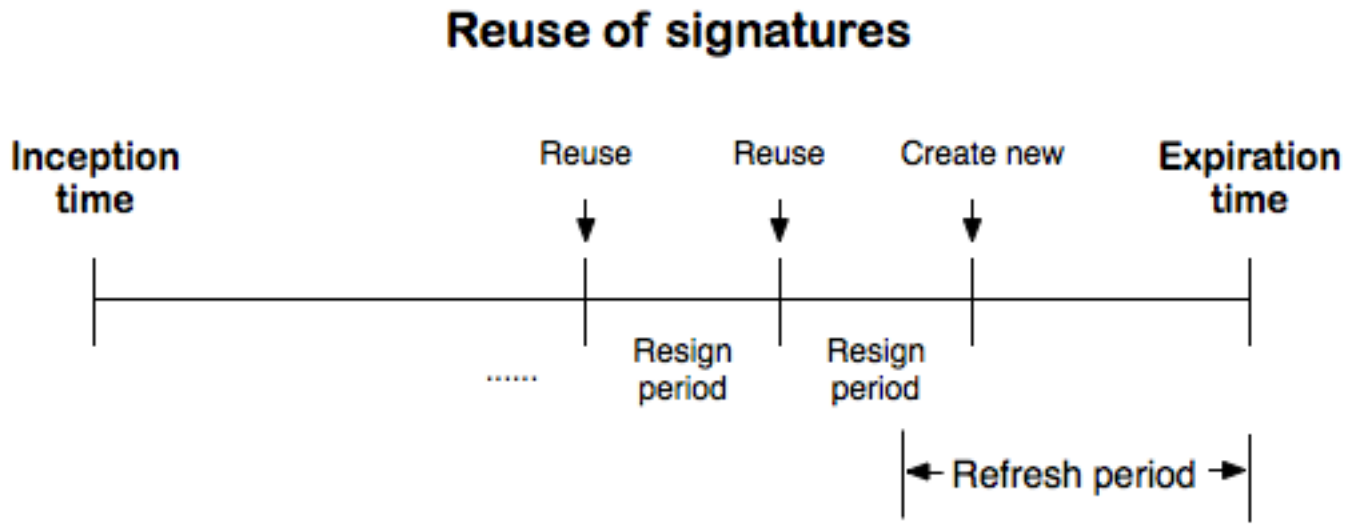
- Signatures are made by keys, and so the ability of a validator to process a signature successfully depends on being able to access the key that made the signature
- All Resource Records in the DNS have timers!
  - TTL is a mandatory field for all records, DNSSEC or not
  - We always have to remember that old records persist in caches
  - A validator will use data from the cache, including DNSKEY, RRSIG, DS
- Signatures have inception and expiration times
  - They are the only records in DNSSEC that contain additional timers
  - Signatures need to be refreshed

Signature Lifetimes (OpenDNSSEC)



https://wiki.opendnssec.org/display/DOCS/kasp.xml

Signature Reuse (OpenDNSSEC)



https://wiki.opendnssec.org/display/DOCS/kasp.xml

Recommended Parameters

- Various guidelines are available
  - RFC 6781, “DNSSEC Operational Practices, Version 2”
  - Software defaults
  - What other TLDs do, e.g. as seen in DNSSEC Policy and Practice Statements
- What should you do?
  - Understand failure modes
  - Choose parameters that suit your operational reality
  - Give yourself plenty of time
  - “Get ahead of the airplane”
    - Be prepared and practice