DNSSEC key rollovers

KINDNS: DNS & DNSSEC operational best practices to improve the DNS Ecosystem



These materials are licensed under the Creative Commons Attribution-NonCommercial 4.0 International license
(http://creativecommons.org/licenses/by-nc/4.0/)



UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Acknowledgements

- This workshop is the latest and greatest attempt at combining the best work of many expert DNS & DNSSEC teachers in our community. It incorporates material from Md Abdul Awal, Philip Paeps, Phil Regnault, Shumon Huque, and unsung heroes at APNIC, ICANN, NSRC, RIPE NCC and probably other organisations.
- Md Abdul Awal deserves all the credit for making a lot of really ugly slides really beautiful, and for correcting hundreds of errors that have persisted for years in previous versions of this material. Thank you!
- Three days are not enough to learn DNS and DNSSEC. After attending this workshop, participants are strongly encouraged to set up their own DNS and get their hands dirty!

Share and enjoy!

These materials are licensed under the Creative Commons Attribution-NonCommercial 4.0 International licence

http://creativecommons.org/licenses/by-nc/4.0/



Please report bugs, errors or omissions.

DNSSEC Key Rollover

- Key rollover limits effects of key compromise
- Typically, ZSKs are rolled over more frequently
  - This can be done transparently, and with no co-ordination with the parent zone
- KSKs are rolled less frequently
  - This does require co-ordinating with the parent zone to sign and install new DS records for the KSKs
- Must keep the chain of trust intact while rolling over the keys

DNSSEC Key Metadata

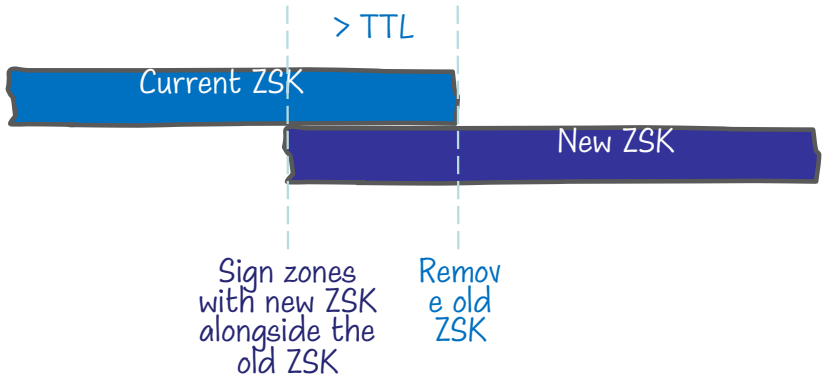
Metadata	Included in Zone File?	Used to Sign Data?	Purpose
Publish	Yes	No	Introducing a key soon to be active
Activate	Yes	Yes	Activation date for new key
Revoke	Yes	Yes	Notifying a key soon to be retired
Inactive	Yes	No	Inactivate or retire a key
Delete	No	No	Deletion or removal of key from zone

ZSK Rollover

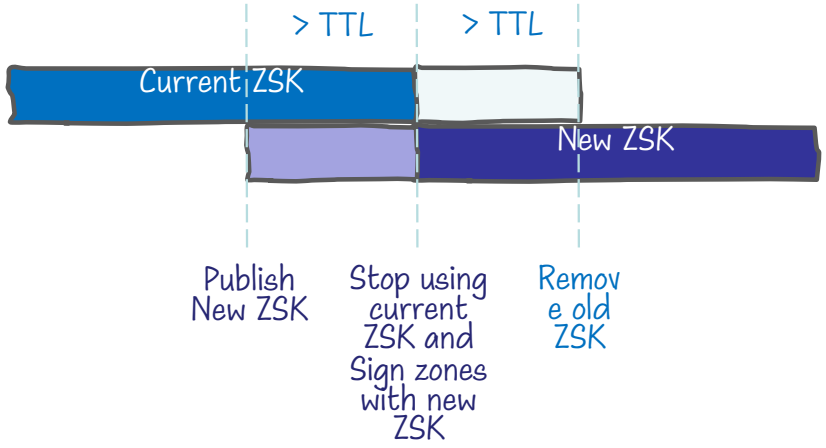
- Double signature
  - Publish the new ZSK and sign the zone with the new key alongside the old one
    - Almost double the size of the zone due to the additional RRSIG for each RRset
  - Wait at least one TTL before removing the old ZSK and old RRSIG.
- Pre-publish
  - Publish the new ZSK into zone data (but do not yet sign zone data with it)
  - Wait at least one TTL so the world's recursive servers know about both keys
  - Stop using the old key and generate new RRSIG using the new key
  - Wait at least one TTL, before removing the old key and re-sign DNSKEY RRset
- The pre-publish tends to be preferred as it doesn't increase the zone size

ZSK Rollover

Double signature Method



Pre-publish Method





KSK Rollover

- Double signature method:
  - Introduce a new KSK in to the DNSKEY RRset
  - Sign the ZSK with both the current ("old") KSK, and the new KSK
  - After sufficient amount of time, substitute the DS record with the new one in the parent zone
  - Sign the zone with only the new KSK
- Pre-publish method:
  - Publish the DS for the new KSK to the parent zone alongside the existing one
  - After a sufficient amount of time has elapsed, replace the current ("old") KSK with the new one and sign the ZSK with the new KSK
- The double signature tends to be preferred as it requires only one interaction with the parent rather than two for each KSK rollover

KSK Rollover

