.TZ KSK Algorithm Rollover

CCNSO, Tech Day
ICANN52 - Singapore
09.02.2015

Simon M. Balthazar

Background

- .TZ zone was signed back in 2012
- Uses Algorithm 5 (RSASHA1)
- Only algorithm supported by the version of the registry software used at the time of implementation
- Adopted OpenDNSSEC for key management
- Upgrade of the registry software in 2014
- First KSK rollover in 2014

Motivation

- Deprecation of SHA1 algorithm as recommended by NIST

- Migration to NSEC3 to prevent zone walking

KSK Rollover Methods

- Double Signature
  - the new KSK is added to the DNSKEY RRset which is then signed with both the old and new key. After waiting for the old RRset to expire from caches, the DS record in the parent zone is changed. After waiting a further interval for this change to be reflected in caches, the old key is removed from the RRset.
- Double DS
  - the new DS record is published. After waiting for this change to propagate into the caches of all validating resolvers, the KSK is changed. After a further interval during which the old DNSKEY RRset expires from caches, the old DS record is removed.
- Double RRset
  - the new KSK is added to the DNSKEY RRset which is then signed with both the old and new key, and the new DS record added to the parent zone. After waiting a suitable interval for the old DS and DNSKEY RRsets to expire from validating resolver caches, the old DNSKEY and DS record are removed

Challenges

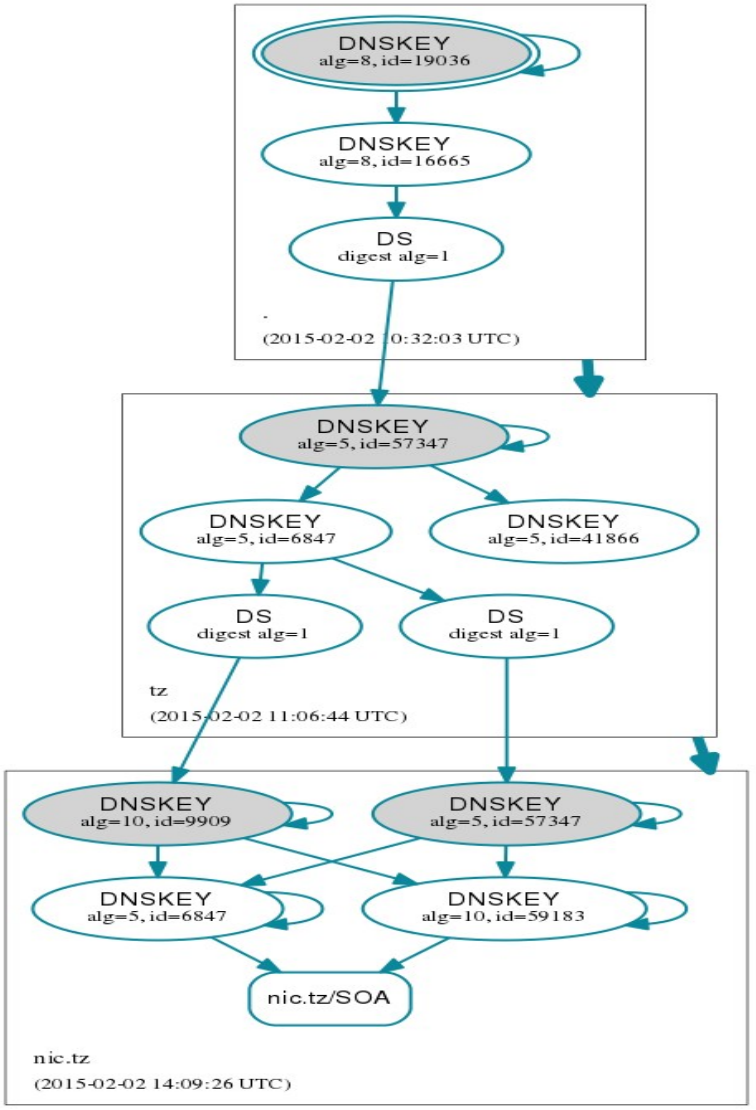
- Algorithm rollover requires simultaneously supporting multiple algorithm. OpenDNSSEC does not support this currently.

- OpenDNSSEC currently does not support Offline KSK.

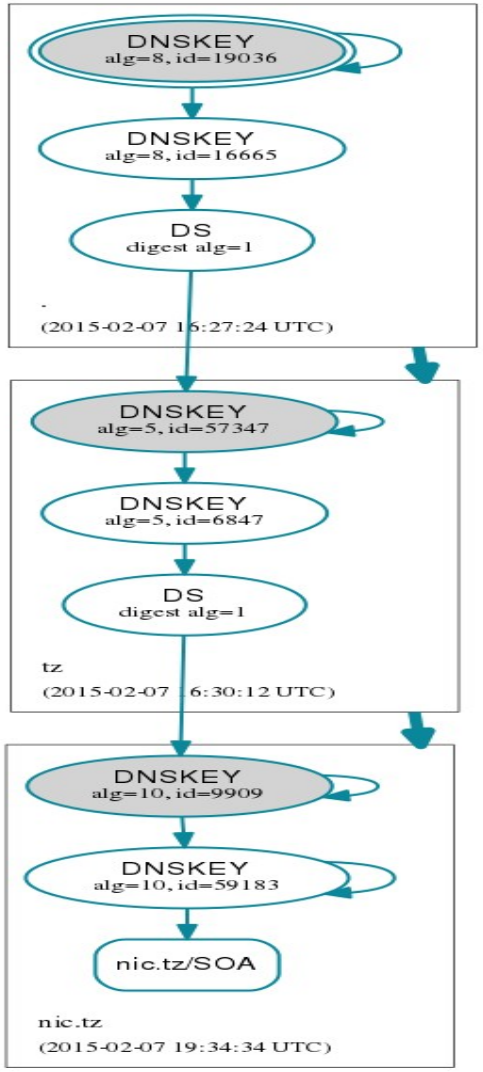
Solution

- Manual process for the algorithm rollover is required using dnssec-signzone.
  - Pre generate a signed zone with double KSK and ZSK signatures using existing keys and the new keys
  - Test on development machine whether the zone still validates using the existing DS in the root/parent zone as well as new DS
  - Publish the new zone
  - Wait for any feedback due to more increased packet size.
  - Continue to update the zone with two signatures (ZSK) as changes comes in.
  - Submit a second DS record for the new algorithm to IANA.

Double RRset for nic.tz



Regular Single Algorithm Zone



- Pre-generate a regular single algorithm zone using the new algorithm
- Swap the new zone in and publish. Wait for feedback
- Ask IANA to remove the old DS. Wait for feedback.

Conclusion

- Two birds One stone!

- This process may allow us to move to the new automated platform smoothly as the new keys may be imported to the newer version of OpenDNSSEC than the one we currently use for keys management

Questions

simon@tznic.or.tz