DNSSEC

.AU Split Key

Adam King
CTO - auDA
June 13 2022

.au Domain
Administration Ltd

.auDA

Why would we do that

- Transitioning the AU zone to 3rd party registry operator
  - auDA operations not staffed to run a registry
- A split offline key would allow auDA to maintain control of the KSK
  - auDA creates and maintains the KSK
  - Registry operator creates and maintains the ZSK
- Keep relationship with IANA/PTI
- Enables smoother transition between registry operators if required
- But it is kind of experimental
  - Very few registries are doing split key

The process

- Were a BIND shop, needed to learn KNOT DNS
  - At the time BIND was not capable of doing offline split key
- Develop and test Key Rollover process and timings
  - Build in time for exchanging keys, errors, corruptions
- Establish Key Signing Request (KSR) / Signed Key Response (SKR) procedures
  - Secure methods for transfer of files
  - Validation of key timings in the file
- New HSM hardware required
  - Registry operator had to move from "DNSSEC in a box" to split signer / HSM
- Matching KNOT DNSSEC policies
  - Split key requires certain parts of the DNSSEC policy to be the same

Testing on testing

- Installation and initial setup began late 2019
  - Off and on focus due to auDA implementation reviews
- New DNSKEY signer setup
  - Registry Operator needed to move to new signers
  - Hampered by Signer failure and replacement parts being shipped during COVID
- BIND and KNOT parameters are very different
  - A lot of testing to understand behaviours
  - Learn and understand different syntax
- Built labs to simulate the “Internet”
  - Root servers, ccTLD servers, 2LD servers, 3LD servers
  - End to end testing
- Use of alternative public domain names
  - Used dnssectest.au to test real world behaviours
  - Establish multiple layered sub domains for end to end testing

Testing on testing (cont)

- Registry operator created side by side signing system
  - Production system running BIND
  - Shadow system running KNOT
- Full life cycle testing
  - Using compressed time frames to test a yearly cycle
  - Manually modifying server time to watch key rollovers in real time
  - Test and evaluate rollover periods
    - How many days is a good balance between identifying a problem and performing an emergency roll without the current key expiring.
- Multiple cutover testing to new system
  - Zone pushed from registry system with manual signing
  - Registry system was still be modified and zone out put manually pushed

Deployment

- Pre-publish of KNOT generated KSK in root zone
  - Get the new KSK DS out in the wild and baked in to resolvers
  - Reduced the TTL (12hrs → 15m) to enable fast transition (and fast roll back if required)
- Removal of other third party slave providers
  - Remove complication and risk
  - Remove requirement to have slave providers pull from new masters
- Cut over completed on 9th March 2022
  - Smooth transition
  - Manual signing as the registry automation piece was not ready
  - Cron jobs for daily resigns
  - No new names being added to the zone
  - Manual SOA roll completed successfully

DNSSEC Outage

- 22 March, 2022 - AU. zone published with missing RRSIG on DNSKEY RRSet.
  - Registry Software zone auto-generation enabled
  - Registry software pushed and incremental update to the signing system for signing and deployment
- Automation failed
  - Due to a bug in signer software the DNSKEY RRSet was dropped
  - KNOT software was unable to reference offline KSK with Incremental transfers
- Quick response
  - auDA and registry operator quickly identified the problem
  - Solution was to manually re-sign the zone
  - DNSKEY RRSet was generated and published
  - Incremental transfers from registry software halted

DNSSEC outage

- Monitoring did not detect issue
  - They way monitoring was configured the missing RRSet was not detected
  - More on this in 2 slides
- We got lucky
  - TTL had been increased to 12 hours (caching helped in this case)
  - Only Cloudflare customers impacted from reports we fielded

Thinking Quickly

- We were about to launch AU Direct and had to think quickly
  - Do we delay, do we manually add records to the zone
  - No appetite to delay the implementation date
- Reached out to CZNIC
  - Spoke with KNOT team who were able to reproduce the problem
  - Very helpful and responsive
  - Had a patch with 24 hours (thank you!)
- Daily updates for 2 days via manual re-signs.
  - Gated the incremental updates from the registry software
  - Merged and manually signed the zone performing validation before publishing
- Knot hotfix
  - Needed testing but all signs were positive
  - Used shadow system again and did zone comparisons
  - Able to promote hotfix on the third day, and resumed automated incremental transfers.

Monitoring

- No gate
  - AU has a tight SLA. 5m from input to registry to publication in the DNS
  - Difficult to perform full zone validation and meet SLA
  - No pre-publish validation was being performed.
- Queries for specific DNSSEC
  - auDA and registry operator monitoring reports the AU zone as ok
  - Checks were run for specific (SOA) signed records (existence and expiry)
  - As these records existed in the zone monitoring was not triggered
  - No top down validation deployed in monitoring stack
- Post-Outage monitoring and Improvements
  - Top down validation checks
  - Local copy of DNSViz used as a monitoring tool
  - Use of drill to validate specific records within the zone
  - Added checks on existence and expiry of DNSKEY RRSIG.

Questions

Thank you

.au Domain
Administration Ltd

.auDA