Offline KSK with Knot DNS 2.8

DNS-OARC 30 - Bangkok

Jaromir Talir • jaromir.talir@nic.cz • 12. 5. 2019
DNSSEC in CZ

- CZ signed in **2006**
  - No HSM
  - Responsibility for key management fully in hands of sysadmins
- Major change in **2013**
  - Split responsibility between sysadmins (ZSK team) and CSIRT (KSK team)
  - KSK goes **offline** into safe
  - Inspired by root zone operations
ZSK operations

- 3 new keys generated every 6 month
  - ZSK rollovers after 2 month
- KSR (Key Signing Request) is prepared and send to KSK team
  - All ZSK combinations prepared for next 6 month as DNSKEY RRsets
  - Signed with PGP of ZSK team
2018126000000-2018126000000_42928_19508_cz.include
2018123100000-2018123100000_19508_42928_cz.include
2018122900000-2019011200000_19508_nnnnn_cz.include
2019011100000-2019012400000_19508_nnnnn_cz.include
2019012200000-2019020500000_19508_nnnnn_cz.include
2019020300000-2019021700000_19508_nnnnn_cz.include
2019021500000-2019022200000_19508_17608_cz.include
2019022000000-2019022700000_17608_19508_cz.include
2019022500000-2019031100000_17608_nnnnn_cz.include
2019030900000-2019032300000_17608_nnnnn_cz.include
2019032100000-2019040400000_17608_nnnnn_cz.include
2019040200000-2019041600000_17608_nnnnn_cz.include
2019041400000-2019042100000_17608_11699_cz.include
2019041900000-2019042600000_11699_17608_cz.include
2019042400000-2019050800000_11699_nnnnn_cz.include
2019050600000-2019052000000_11699_nnnnn_cz.include
2019051800000-2019060100000_11699_nnnnn_cz.include
2019053000000-2019061300000_11699_nnnnn_cz.include

; This is a zone-signing key, keyid 19508, for cz.
cz. IN DNSKEY 256 3 13 PoL4KRw/
BLPZfko4BxjmX89Vu5SVyln4pNYhktK9VRw+CnUlFd80+hPG
l0LhIXT10BBYhVw40aEp6BWu/cvhWQ==

; This is a zone-signing key, keyid 42928, for cz.
cz. IN DNSKEY 256 3 13
GrWu3AwLX3b2yEVeTN4wVllu7Kay3roEADrhYloX9Y+KpJEqVp3gTt/
eKBZboTl2pFy2rZFuFPGDZWAoL1IGg==

; This is a zone-signing key, keyid 19508, for cz.
cz. IN DNSKEY 256 3 13 PoL4KRw/
BLPZfko4BxjmX89Vu5SVyln4pNYhktK9VRw+CnUlFd80+hPG
l0LhIXT10BBYhVw40aEp6BWu/cvhWQ==
KSK operations

- KSK environment is laptop w/o wifi, fixed bootable image and private part of KSK in the safe
- Signing ceremony is held with multiple witnesses and signed report
- SKR (Signed Key Response) is created, signed with PGP of KSK team and sent back to ZSK team
SKR generation

- Public part of KSK appended to each DNSKEY RRset
- DNSKEY RRsets transformed to zonefiles
- Zonefiles are signed with KSK
- DNSKEY and RRSIG records extracted from zonefiles
Zone signing

- Unsigned zone is generated every 30min
- Set of checks is applied to verify content
- Appropriate SKR file (based on time) is included into zonefile
- Signatures from previous signing are included as well to speed up signing
- Zone is signed with ZSK based on the tag in the filename
Toolbox

- Set of shell scripts around:
  - dnssec-keygen
  - named-checkzone
  - ldns-compare-zones
  - dnssec-signzone
  - named-compilezone
  - ldns-read-zone
Challenges

- Algorithm rollover modifications
- Manual backup & HA
- Scripts are aging
- Staff is changing
- Who should be responsible for scripts? Registry development team or sysadmins?
Challenges

- Why the hell CZ.NIC’s signer is Bind and not Knot DNS?
- Can we switch to automated signing?
- No support for automated signing with offline KSK in DNSSEC signer implementations
Way forward

- Sysadmins and Knot DNS developers worked together to collect requirements
- Offline KSK support implemented in Knot DNS 2.8 released few months ago
Knot DNS & DNSSEC

- Authoritative DNS server with automated DNSSEC signing
  - Just set the policy and you can forget DNSSEC
- Accepts also DNS transfers on input - can serve as “bump-in-the-wire” signer
- Full DNSSEC feature set:
  - PKCS11, CDS/CDNSKEY, Shared KSK, Algorithm rollover, Combined Signing Key, ...
Knot DNS & DNSSEC

- RIPE NCC selected Knot DNS as DNSSEC signer of their choice 6 months ago
  - 116 zones
  - Update will be presented at RIPE 78
- DNSSEC signer performance study by DK Hostmaster
  - Will be presented at CENTR TechWG
Automated signing

policy:
- id: my_policy
  algorithm: ECDSAP384SHA384
  zsk-lifetime: 60d

zone:
- domain: example.com.
  **dnssec-signing: on**
  dnssec-policy: my_policy
Offline KSK signing

policy:
- id: my_policy
  algorithm: ECDSAP384SHA384
  zsk-lifetime: 60d
  manual: on
  offline-ksk: on

zone:
- domain: example.com.
  dnssec-signing: on
  dnssec-policy: my_policy
Offline KSK signing – ZSK team

- Pregenerate ZSKs for next 6 month

  $ keymgr -c zsk-team.conf example.com. pregenerate +6mo

- Create KSR

  $ keymgr -c zsk-team.conf example.com. generate-ksr +0 +6mo > ksr
Offline KSK signing – KSR

;; KeySigningRequest 1.0 1544709874 ===========
example.com. 5 DNSKEY 256 3 14
PVP1IF7CtEu3+BiERm4jvZ0LaboxY0jSrb69gpaY5RJhIsuazjekjPQRIFGUMnH7LMH+TWRFM1Zz5zpk
4C0p1QfaTPcdOzOuis+QsfCftsrd5J7JprPQz22C+H2rt8qf

;; KeySigningRequest 1.0 1544710698 ===========
example.com. 5 DNSKEY 256 3 14
PVP1IF7CtEu3+BiERm4jvZ0LaboxY0jSrb69gpaY5RJhIsuazjekjPQRIFGUMnH7LMH+TWRFM1Zz5zpk
4C0p1QfaTPcdOzOuis+QsfCftsrd5J7JprPQz22C+H2rt8qf

;; KeySigningRequest 1.0 1544710763 ===========
example.com. 5 DNSKEY 256 3 14
/P5l3LxwUhcDB7CwLolL5OmWCV+TcMzudehZVlt8QKn7DcxXYaKoabrN0jXtPhpyZ4cPE+/
UMpT+008cTqrNr1luqFxUWyHKeEzrYUB9FirmSMHM22z2CugQZ+KuLkxc

;; KeySigningRequest 1.0 1544710828 ===========
example.com. 5 DNSKEY 256 3 14
/P5l3LxwUhcDB7CwLolL5OmWCV+TcMzudehZVlt8QKn7DcxXYaKoabrN0jXtPhpyZ4cPE+/
UMpT+008cTqrNr1luqFxUWyHKeEzrYUB9FirmSMHM22z2CugQZ+KuLkxc

;; KeySigningRequest 1.0 1544711074 ===========
Offline KSK signing – KSK team

- On the first usage generate KSK (or import)
  
  $ keymgr -c ksk-team.conf generate

- Sign KSR during ceremony
  
  $ keymgr -c ksk-team.conf example.com. sign-ksr ksr > srk
Offline KSK signing – SKR

;;; SignedKeyResponse 1.0 1544709874 ===========
example.com. 5 DNSKEY 256 3 14
PVP1IF7CtEu3+BiERm4jvZ0LaboxY0jSrb69gpaY5RJhlSuazjekjPQRIFGUMnH7LMH+TWRFM1Zz5z
pk4C0p1QfaTPcdOzOuis+QsfCftsr57JPrPQz22C+H2rt8qf
example.com. 5 DNSKEY 257 3 14
eTcVgRXNDrZGLYvHkVu/e8uAIHjL4HdYkQdMlh/top2tnaVAmgaXCvr8BtgGDFLKy84DcCYTMtzzSl8
uzB5ef/ZZWH2QHFygYT03NTlluUqxcfYe3ycQ0u5DzL2YYS
example.com. 5 RRSIG DNSKEY 14 2 5 20181213140634 20181213123434 11919
example.com. qJuUZYqHt1N5YDnh4/Qp7Ic4FBC6lX10tRR/ZDPul+V3znIfyiqrMDjDhT5+tVYsr/
0iycls604gWpdMUTS1OUE8+nUSW3dqXqr8hv7P0o9/S88le//eiMi1JcYKPA

;;; SignedKeyResponse 1.0 1544710698 ===========
example.com. 5 DNSKEY 256 3 14
PVP1IF7CtEu3+BiERm4jvZ0LaboxY0jSrb69gpaY5RJhlSuazjekjPQRIFGUMnH7LMH+TWRFM1Zz5z
pk4C0p1QfaTPcdOzOuis+QsfCftsr57JPrPQz22C+H2rt8qf
example.com. 5 DNSKEY 256 3 14
/5l3LxwUhcDB7CwLoll5OmWCV+TcMzudehZVlt8QKn7DcxXYaKoabrN0jXtPhypzy4cPE+/
UMpIT+008cTqrNrluqFxUWYPHeEzrYUB9FirnSMHM22z2CugQZ+KulKxc
example.com. 5 DNSKEY 257 3 14
eTcVgRXNDrZGLYvHkVu/e8uAIHjL4HdYkQdMlh/top2tnaVAmgaXCvr8BtgGDFLKy84DcCYTMtzzSl8
uzB5ef/ZZWH2QHFygYT03NTlluUqxcfYe3ycQ0u5DzL2YYS
example.com. 5 RRSIG DNSKEY 14 2 5 20181213142018 20181213124818 11919
example.com.

CrPvdWwkCnYiirqhFOLW9npkW92tmuf2Nz3UM/MM1+/7dCvbslmoD0hw+skaMItlvw8F34SV8wvmD11uZL8E8+b3RFgNT5iAei4mXScQpF5VfWp2CMXFzkeMVnGk77FZ+

;;; SignedKeyResponse 1.0 1544710763 ===========
Offline KSK signing – ZSK team

- Import output from KSK team
  
  $ keymgr -c zsk-team.conf example.com. import-skr skr

- Inform knot daemon to refresh state
  
  $ knotc -c zsk-team.conf zone-sign example.com.
Knot DNS 2.8 – other features

- Configurable multithreaded DNSSEC signing for large zones
- New 'double-ds' option for CDS/CDNSKEY publication
- New knotc trigger 'zone-key-rollover' for immediate DNSKEY rollover
- ... and many more
Future

- Testing, testing, testing…
- Hopefully migration of CZ will finish this year
- Any other TLD operating similar way?
Thank You

Jaromir Talir • jaromir.talir@nic.cz • https://www.nic.cz
https://www.knot-dns.cz/