

Technical Parameter Decisions for DNSSEC



By
Mark Elkins
July 2013



DNS
Domain Name Services (Pty) Ltd

ZSK - Zone Signing Keys



- Its a security key - use secure algorithms
- Create it to be flexible in use
- Its a security key - longer keys are more secure
- Used to sign almost all the data in a zone - so should not be long
- Because its not long - should be changed reasonable frequently
- Can not change too frequently - to allow for key roll-over

Current wisdom: `dnssec-keygen -a RSASHA256 -b 1024 <zone>`

Length: 1024 bits

Life span: One Month

Algorithm: RSASHA256

Usage: Both NSEC and NSEC3



KSK - Key Signing Key



- Its a security key - use secure algorithms
- Create it to be flexible in use
- Its a security key - longer keys are more secure
- Used to sign only a little data - long is fine
- Because its long - can be changed less frequently

Current wisdom: `dnssec-keygen -a RSASHA256 -b 2048 -f KSK <zone>`

Length: 2048 bits

Life span: One Year

Algorithm: RSASHA256

Usage: Both NSEC and NSEC3



Zone signing NSEC or NSEC3



NSEC allows a zone to be walked - does this matter?

Small zone with well known information

'za' tld (18 records),
most small websites
reverse IPv4 zone

NSEC3 'hides' the zone content

Large zone with "confidential" information

'co.za' secondary-tld (almost a million records)
large company zones
reverse IPv6 zone



NSEC3 Parameters



- Opt in/Opt out
- Hash count
10 or less
- Prefix,
size - 4 bytes
Regular changes - two weeks



Collecting Keys

- EPP
- Secure Web
- Other

Does the parent require DS or DNSKEY records



Signing Platform



Software choices

- OpenDNSSEC 
-  DNSSEC-Tools
- Roll-your-own with BIND 

Signature storage

- File System 
-  **SoftHSM** (Hardware Security Module)
- HSM appliance (May also sign zone) 