Key maintenance

- At the name server
  - Key generation
  - Zone signing
  - Key rollover
  - Secure delegation
- At the resolver
  - Updating trust anchors

Key generation

- Key options
  - ZSK, KSK
- Algorithm support
  - RSASHA1, DSA
- Key length
- Entropy source
- Examples:
  - dnssec-keygen, jdnssec-keygen, ldns-keygen, pdnssec-keygen, maintkeydb, ...

Zone signing

- Zone signing vs. Key signing

- NSEC3 support

- Examples:
  - dnssec-signzone, jdnssec-signzone, ldns-signzone, pdnssec-signzone, dnssigner, Zonesigner, ...

Key rollover

- ZSK rollover

  – Pre-publish key rollover

- KSK rollover

  – Double signature rollover

- Examples:

  – Rollerd, maintkeydb, ...

Secure delegation

- Create DS records
  - dnssec-dstool, dnssec-signzone, ldns-key2ds, Key2ds, ...

- No real in-band solution for DS registration at the parent.

Trust anchors

- Automated Updates of the DNSSEC Trust Anchors: RFC 5011

- Examples:
  - Trustman, autotrust, ...

NLnet
Labs

Troubleshooting

- Zone verification:
  - Donuts, jdnssec-verifyzone, ldns-verify-zone, named-checkzone, ...

- Debugging:
  - dig, drill, validate, dnspktflow, dnsdump, dnscap, Logwatch, ...

Developer resources

- Libraries
  - libval & libsres, ldns, libunbound, ...

- Perl SDKs
  - Net::DNS::SEC

- Validator API
  - DNSSEC Validator
  - libunbound

Overview

- Lots of choice

- Aid vs. automation

- Efforts 'DNSSEC in a box'
  - DNS Signer (Secure64)
  - DNSx (Xelerance)