Trust History

• Draft-wijngaards-dnsop-trust-history -01
• Support validators for end-users
  – Offline for long periods
  – Software years on the shelf
• Make old trust anchor up to date
  – Over port 53 because that works at system start
  – Security is similar to 5011: spoofs, key, 30days
• History list of key sets and old signatures
Update in 4 easy steps

1. Fetch current keyset
   - If no successful key use in 30 days

2. Get list head
   - Location in the validator configuration

3. Walk through list
   - Check if SEP key (a KSK) signs the next keyset
   - Checks trust point revocation and algorithm rollover

4. If keyset is signed by your (old) trust anchor
   - Store end result on stable storage
TALINK

- Dnsext expert review RR Type allocation
- RDATA contains 2 domain names
  - `<listhead> IN TALINK <first> <last>`
  - `<listitem> IN TALINK <prev> <next>`
  - Empty label '.' denotes end-of-list or empty list
- Uncompressed names in the wireformat