Trust History
Update in 4 easy steps

1. Fetch current keyset
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

• Dnsxt expert review RR Type 58 (dec)
• 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
dnsop-dnssec-trust-history-01

• Documented security choice (after discussion with Joe Abley)
  – Lifetime on keys, if expired you choose:
    • No connectivity
    • No DNSSEC
    • Out of band software-update (if you have it)
  – No lifetime, 'better than nothing' security

• No 30-day wait if not using rfc5011
  – To be able to follow regular rollovers
  – SHOULD warn operator of changed keys