Automated (DNSSEC) Child Parent Synchronization using DNS UPDATE

Matthijs Mekking
draft-mekking-dnsop-auto-cpsync
History

• Originated at IETF75, Stockholm
  – Informal dnssec-discuss gathering
• Goal: fully automate DNSSEC operations
First Approach

• Pull Method
  - Parent polls child to see if the DNSKEY RRset has changed
  - Child can NOTIFY
  - Authentication with DNSSEC

• Drawbacks
  - Parent creates DS record
  - No emergency key rollover
  - Does not work in the RRR model
Current Approach

• What about the push method?
  - Child sends UPDATE when there is a new DS (extended use of DNS UPDATE)
  - TSIG/SIG0 authenticated
  - Take care of granting privileges
  - Can also be used to update other records at the zone cut (NS, glue)
  - Possible to send UPDATE to a proxy
Current Approach

- Child can create DS record itself
- Also covers emergency key rollover
- It works in a RRR environment
Open Issues

• Concerns about scalability of TSIG
• Service discovery mechanism
• 'Narrow' glue records
• The role of the registrar
http://www.ietf.org/id/draft-mekking-dnsop-auto-cpsync-00.txt