Limitations, Goals & Requirements for delegations

Roy Arends @ IETF119

ICANN

DD

Limitations of legacy delegations

- No method to signal capabilities
  - such as secure transport
- Operator dependency on the Registrant/Registrar/Registry chain
  - for any change to the NS/DS set
- NS and Glue records are not signed in the parent zone
  - They may be signed elsewhere but can only be verified after the delegated (child) zone is contacted
- Parent/Child inconsistency
  - Lack of standard language, resolver may be child or parent centric, or even sticky. Has lead to confusion, misconfiguration, and security problems

Goals for Designing a New Delegation Method

- Facilitate Nameserver Capabilities
  - Secure transport, error reporting, new encodings, etc
- Outsource Operations
  - Parent (or RRR) Independent Operations, including DS management.
- Nameserver authentication
  - Verify before use.
- Extensible
  - Your future method goes here...

Requirements for a New Delegation Method

- Cryptographic Security against downgrade attacks
  - DELEG Removal must be detectable
    - Auth servers MUST include an NSEC/NSEC3 proving absence of DELEG.
    - Resolvers MUST expect an NSEC/NSEC3 proving absence of DELEG.
    - For future parent side delegation records, always include NSEC/NSEC3.
  - a DNSKEY flag can indicate that a resolver must expect NSEC/NSEC3.
- Backwards Compatibility
  - New delegation methods should not break existing implementations
    - All major implementations ignore unknown records and DNSKEY flags

Food for thought

- Future safe: Dedicate a range of record types as parent side only, so authoritative servers can include them as is (without the need to interpret them)
- NS+Glue support has a long tail due to legacy implementations.
- More inconsistency: DELEG, Parent/child NS, Glue can all mismatch.
- DS Aliasing requires a bridge of trust. There needs to be a chain of trust between:
  1. a trust anchor and the parent that does the aliasing.
  2. a trust anchor and the alias.