draft-dns-zone-digest

IETF 104 Prague

TL;DR

- Secure zone files no matter how they are distributed
  - This is about data security
  - It is not about channel security
- Cryptographic digest (hash) of zone data
- Digest added to zone data – ZONEMD RR type
- Preferably secured by DNSSEC

https://datatracker.ietf.org/doc/draft-wessels-dns-zone-digest/

Changes since -02

- Standards Track -> Experimental
- ZONEMD digest types have their own IANA registry
- SHA384 only defined ZONEMD digest type
- Added Reserved field
- RR type 63 allocated by IANA
- Various clarifications and corrections
- -06 is current

Large Dynamic Zones

- For large, dynamic zones it is prohibitive to frequently re-digest the entire zone
- Merkle Trees can significantly improve performance for this situation
- Propose a Reserved field for encoding Merkle Tree depth and future experimentation
- Initial specification works with moderate / stable zones
- Future specification works with large, dynamic zones with no change to RDATA

For discussion: Number of ZONEMD records

- Draft currently restricts ZONEMD to one per zone
  - More correctly: one ZONEMD RR at the apex
- Allowing multiple ZONEMD enhances algorithm agility
- But makes downgrade attacks a concern
- Would need to define verification given multiple ZONEMDs
  - All?
  - Any one?
  - Receiver’s choice?

For discussion: Allow ZONEMD below apex?

- Should ZONEMD be restricted to the apex, like SOA?
- Non-apex ZONEMDs could be otherwise ignored.

Scope of Experimentation

- Allow community time to analyze and evaluate ZONEMD
- Conduct experiments with variable-depth Merkle trees
  - Encoded in Reserved field

Implementations

- https://github.com/verisign/ldns-zone-digest
- https://github.com/shane-kerr/ZoneDigestHackathon

See also

- https://indico.dns-oarc.net/event/29/contributions/656/

Questions?