draft-dns-zone-digest

IETF 102 Montreal

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 (all) zone data
- Digest added to zone data – ZONEMD RR type
- Preferably secured by DNSSEC

Motivation / Use Case

- Root zone spreading beyond traditional deployment boundaries
  - RFC 7706
  - Talk of “hyper-local root” in ICANN contexts

Non-Use Case

- Very large zones
  - .COM
- Very dynamic zones
- Although perhaps still useful for ICANN Centralized Zone Data Service (CZDS)?

Why not just use PGP?

- Detached signatures only weakly associated with the data they cover
- Attached signatures change the file format (no longer a zone file)
  - Lost when zone is loaded into a name server
- Would require DNSSEC to associate a PGP key with a zone
  - or web-of-trust (yeah right)
- Digest is marginally useful even without DNSSEC
- Unlikely that name server implementations would incorporate PGP
  - Whereas DNSSEC is already there

Simple example

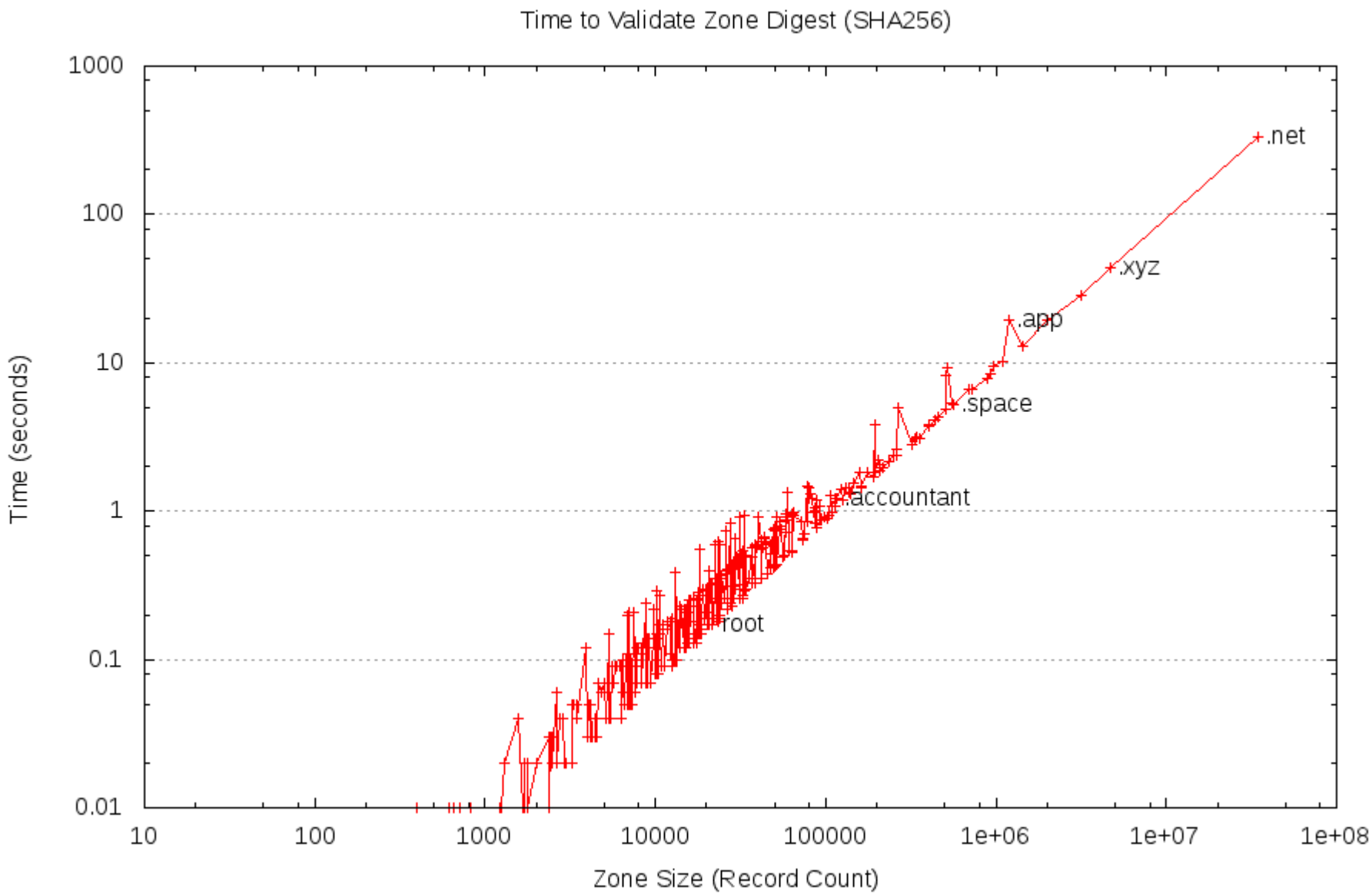
```
example.  86400 IN A       127.0.0.1
example.  86400 IN NS      ns.example.
example.  86400 IN SOA     ns.example. admin.example. (
                              2018031900 1800 900 604800 86400 )
example.  86400 IN ZONEMD  2018031900 2 (
                              470e532450143fcae448942cd530e3d7
                              9a303cea62e4c930f2102becb4fe68d8 )

ns.example.   3600 IN A       127.0.0.1
```

Dynamic Updates

- ZONEMD as proposed requires full hash calculation on every change
  - not designed for rapid dynamic DNS updates
  - Digest can be easily calculated where DNSSEC offline signing is used
  - Not designed for dynamic / online signing / minimal-NSEC

- Supporting dynamic digest update could be defined by future protocol enhancement
  - Perhaps with Merkle trees / hierarchical hashing
  - Perhaps under a different RR type


Time to Validate Zone Digest (SHA256)
Time (seconds)
1000
100
10
1
0.1
0.01
10
100
1000
10000
100000
1e+06
1e+07
1e+08
Zone Size (Record Count)
.net
.xyz
.app
.space
.accountant
root

Algorithm for Calculating Digest

- Add placeholder ZONEMD record
- Sort and canonicalize zone
- Optionally sign with DNSSEC
- Calculate digest and update ZONEMD record
- Update ZONEMD RRSIG if signed