Deploying ZONEMD in the Root Zone

Duane Wessels

DNS-OARC 41, September 6, 2023

Reminder – What is ZONEMD?

- RFC 8976 “Message Digests for DNS Zones”
- A cryptographic digest, or hash, of the data in a DNS zone
- Embedded in the zone data itself as ZONEMD resource record
- Computed by zone publishers
- Verified by zone recipients

Coming Soon to the Root Zone

- September 13, 2023
  - DURZ II -- Deliberately Unverifiable Root ZONEMD
  - ZONEMD record published with private use Hash Algorithm (241)
  - Hash value will be remarkably similar to SHA-384
- December 6, 2023
  - ZONEMD Hash Algorithm will change to SHA-384

ZONEMD in the Root Zone

- Root zone's first new record type in 13 years!
- On ftp.internic.net and www.internic.net it will appear in native presentation format:

```
.       86400   IN      ZONEMD  2023050202 1 1
7706681eadb4bb5a84b109a43fc72a2a35f8bc6752a27040
e51d926af47603568a4d6c8fd6395d4e9a2c9b89a5599783
```

Implementations

Implementation	Parse	Publish	Verify	Notes
ldns-zone-digest	✅	✅	✅	RFC reference implementation
Unbound	✅	❌	✅	v1.13.2; *auth-zone* stanza
ldns	✅	✅	✅	*ldns-signzone* and *ldns-verifyzone*
NIC Chile dns-tools	✅	✅	✅	implemented in Go
NSD	✅	❌	✅	external verifier
PowerDNS Recursor	✅	❌	✅	v4.7.0, ”Zone to Cache”
Knot DNS	✅	✅	✅	v3.1.0
Knot Resolver	✅	❌	❌	waiting for ZONEMD in root
BIND9	✅	❌	❌	further work in progress
Perl Net::DNS	✅	❌	❌	parse only
YAZVS	✅	❌	✅	Yet Another Zone Validation Script
OpenDNSSEC	✅	✅	?	Soon to be released

Additional Information

- RFC 8976: “Message Digests for DNS Zones”
- RZERC 003: “Adding Zone Data Protections to the Root Zone”
- Root Server Operators Statement on adding ZONEMD to the root zone
- Verisign Blog: “Adding ZONEMD Protections to the Root Zone”
- APNIC Ping Podcast episode “Adding ZONEMD protections to the root zone”

- Announcements to be made on the dns-operations list.

VERISIGN®