Draft Plan for Deploying ZONEMD in the Root Zone

Table of Contents

Background

Message Digests for DNS Zones (RFC 8976) describes a protocol and new DNS Resource Record that provides a cryptographic message digest over DNS zone data at rest. The ZONEMD Resource Record conveys the digest data in the zone itself. When used in combination with DNSSEC, ZONEMD allows recipients to verify the zone contents for data integrity and origin

authenticity. This provides assurance that received zone data matches published data, regardless of how the zone data has been transmitted and received.

The root zone is one of the most widely distributed DNS zones on the Internet, served by more than 1400 separate Root Server instances[1] at the time of this writing. Additionally, many organizations configure their own name servers to serve the root zone locally. Reasons for doing so include privacy and reduced access time. RFC 8806 describes one way to do this. As the root zone spreads beyond its traditional deployment boundaries, the verification of the completeness of the zone contents becomes more important.

This document describes a plan to add ZONEMD to the root zone. It has been jointly developed by Verisign as the Root Zone Maintainer, and by ICANN as the IANA Functions Operator.

Impacted Components and Parties

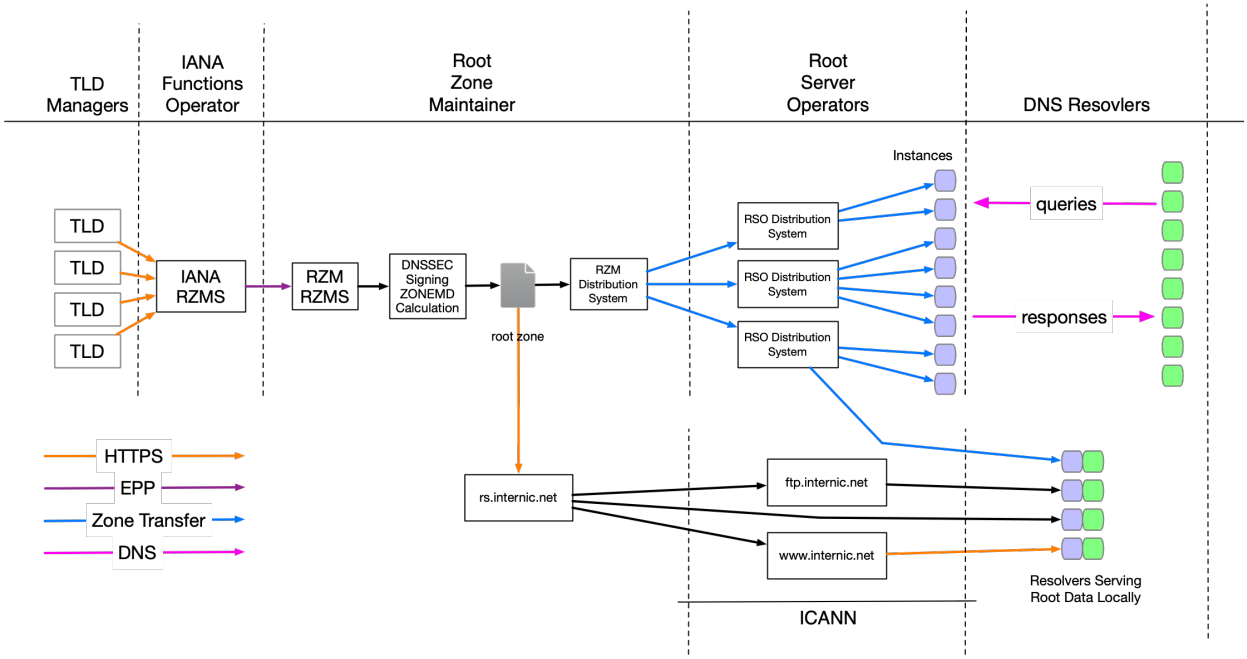

Figure 1 Components involved in root zone provisioning, distribution, and resolution.

TLD Managers

TLD Managers that interact with IANA for root zone changes are not impacted by plans to add the ZONEMD record to the root zone.

IANA RZMS

IANA's Root Zone Management System is not impacted by plans to add the ZONEMD record to the root zone.

[1] https://root-servers.org/

Verisign RZMS & Distribution System

Verisign's Root Zone Management System is being updated to support the ZONEMD record. The components that are responsible for signing the root zone with the Zone Signing Key will also calculate the digest and add the ZONEMD record to the zone data.

Verisign's root zone distribution systems have been verified to operate correctly on zones that include the ZONEMD record.

Root Server Operators

The Root Server Operators are ensuring that their internal zone distribution systems and name servers can support the ZONEMD record. RSOs are not required to enable ZONEMD verification. Rather, they are simply confirming that the mere presence of the ZONEMD record does not negatively impact their operations.

Traditional Recursive Resolvers

Recursive resolvers on the internet are not impacted by plans to add the ZONEMD record. There is no expectation that resolvers will issue queries for the ZONEMD record, and there is no harm should they do so.

Recursive Resolvers Serving Root Data Locally

Recursive Resolvers that have been configured to serve root data locally (e.g., as in RFC 8806) may perform ZONEMD verification by default. Unbound version 1.13.2[2] will perform ZONEMD verification.

internic.net services

The root zone and other data is made available to the public on web and file transfer services operating under the internic.net domain. Since these services simply treat the information as an opaque file, they are not impacted by plans to add the ZONEMD record to the root zone.

Users of internic.net services

Users that download the root zone from an internic.net service may be impacted by the addition of the ZONEMD record. It is possible that users are downloading and reading the root zone file, perhaps using automated processes. If the tools used to read and parse the root zone are unaware of the ZONEMD record, processing may fail.

[2] https://www.nlnetlabs.nl/news/2021/Aug/12/unbound-1.13.2-released/

Operational Considerations

Hash Algorithm

RFC 8976 defines two hash algorithms for use in ZONEMD records: SHA-384 and SHA-512. The SHA-384 algorithm produces digests of size 384-bits, or 48 octets. Similarly, SHA-512 produces 512-bit digests, or 64 octets. The RFC also reserves a number of hash algorithm code points for private use.

Although the longer digest would be cryptographically preferable, SHA-384 has been selected for the initial implementation for compatibility reasons.

Internet Systems Corporation, the developers of BIND, implemented ZONDEMD based on an early Internet Draft from February 2019. At that time the proposed ZONEMD record placed the hash algorithm in the record's second field, and only SHA-384 was defined. Later the meanings of the ZONEMD fields were changed. The hash algorithm moved to the third field and SHA-512 was added. Versions of BIND from the initial implementation, which are in relatively widespread use today, experience errors when encountering a SHA-512 ZONEMD record. This is due solely to the amount data found in the digest field, and not the value present in the hash algorithm field. The issue was fixed in April 2021 and released in BIND versions 9.11.32, 9.16.16, and 9.17.13.

Presentation Format

Distribution of the zone between the Root Zone Maintainer and Root Server Operators primarily takes place via the DNS zone transfer protocol. In this protocol, zone data is transmitted in "wire format."

The root zone is also stored and served as a file on the internic.net FTP and web servers. Here, the zone data is in "presentation format."

Some consumers of zone data received from the FTP and web servers might currently be using software that does not recognize the ZONEMD presentation format. In other words, such software may fail to parse a record like this:

```
. 86400 IN ZONEMD 2021101902 1 1
7d016e7badfd8b9edbfb515deebe7a866bf972104fa06fece85402cc4ce9b69bd0cbd65
2cec4956a0f206998bfb34483
```

However, older software is more likely to parse the equivalent record in the unknown, or generic format as defined in RFC 3597:

```
. 86400 IN TYPE63 \# 54
7877914e01017d016e7badfd8b9edbfb515deebe7a866bf972104fa06fece85402cc4ce
9b69bd0cbd652cec4956a0f206998bfb34483
```

For this reason, in the initial implementation, the ZONEMD record shall appear in the unknown / generic format on the internic.net servers.

Phased Approach

In the interest of proceeding with caution, the ZONEMD record in the root zone shall be introduced in two phases.

The first phase shall use a private-use hash algorithm number. This makes the ZONEMD digest unverifiable and allows impacted parties to ensure that the mere presence of the ZONEMD record does not cause problems.

In the second phase, the hash algorithm will be changed to SHA-384. At this point the ZONEMD record becomes verifiable.

Technical Correctness Checks

Each root zone generated by the Verisign is subject to several technical checks prior to publication. Verisign is adding two new ZONEMD verification checks as part of its changes to RZMS, each having diverse authorship and diverse programming languages.

If any ZONEMD verification check fails, the candidate root zone enters a holding state and will not be published. Verisign staff will manually check the zone for correctness and take appropriate action.

Deployment Schedule

Prerequisites

Prior to adding any ZONEMD record to the root zone, Verisign must implement and deploy changes to its Root Zone Management System. This work is expected to be complete by Q2 2022.

All Root Server Operators must confirm their readiness for the ZONEMD record.

Phase one

The first phase may begin once all prerequisites have been satisfied, and when ICANN instructs Verisign to begin publishing a ZONEMD record with a private use algorithm. This phase is expected to begin in Q2 2022 and last for approximately two months.

If any significant problems are encountered during phase one that are attributable to the presence of the ZONEMD record, Verisign and ICANN may agree to revert to publishing the root zone without a ZONEMD record.

Phase two

The second phase may begin approximately two months after the start of phase one. When instructed by ICANN, Verisign will begin publishing a ZONEMD record with the SHA-384 hash algorithm.

If any significant problems are encountered during phase two that are attributable to the ZONEMD record, Verisign and ICANN may agree to revert to publishing the root zone without a ZONEMD record.