Message Digest for DNS Zones
draft-ietf-dnsop-dns-zone-digest-02

Abstract

This document describes an experimental protocol and new DNS Resource Record that can be used to provide a message digest over DNS zone data. The ZONEMD Resource Record conveys the message digest data in the zone itself. When a zone publisher includes an ZONEMD record, recipients can verify the zone contents for accuracy and completeness. This provides assurance that received zone data matches published data, regardless of how the zone data has been transmitted and received.

ZONEMD is not designed to replace DNSSEC. Whereas DNSSEC protects individual RRsSets (DNS data with fine granularity), ZONEMD protects a zone’s data as a whole, whether consumed by authoritative name servers, recursive name servers, or any other applications.

As specified at this time, ZONEMD is not designed for use in large, dynamic zones due to the time and resources required for digest calculation. The ZONEMD record described in this document includes fields reserved for future work to support large, dynamic zones.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."
time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 30, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction ............................................. 3
   1.1. Motivation ........................................ 4
   1.2. Design Overview ................................... 5
   1.3. Use Cases .......................................... 6
       1.3.1. Root Zone .................................. 6
       1.3.2. Providers, Secondaries, and Anycast .......... 6
       1.3.3. Response Policy Zones ........................ 7
       1.3.4. Centralized Zone Data Service ............... 7
       1.3.5. General Purpose Comparison Check ............ 7
   1.4. Requirements Language .............................. 7
2. The ZONEMD Resource Record .............................. 7
   2.1. ZONEMD RDATA Wire Format ......................... 8
       2.1.1. The Serial Field ............................ 8
       2.1.2. The Digest Type Field ..................... 8
       2.1.3. The Parameter Field ....................... 8
       2.1.4. The Digest Field ........................... 9
   2.2. ZONEMD Presentation Format ...................... 9
   2.3. ZONEMD Example ................................... 9
3. Calculating the Digest .................................. 9
   3.1. Canonical Format and Ordering .................... 9
       3.1.1. Order of RRSets Having the Same Owner Name . 10
       3.1.2. Duplicate RRs .............................. 10
   3.2. Add ZONEMD Placeholder .......................... 10
   3.3. Optionally Sign the Zone ........................ 10
   3.4. Calculate the Digest ............................ 11
       3.4.1. SHA384-STABLE Calculation ................... 11
1. Introduction

In the DNS, a zone is the collection of authoritative resource
records (RRs) sharing a common origin ([RFC7719]). Zones are often
stored as files on disk in the so-called master file format
[RFC1034]. Zones are generally distributed among name servers using
the AXFR [RFC5936], and IXFR [RFC1995] protocols. Zone files can
also be distributed outside of the DNS, with such protocols as FTP,
HTTP, rsync, and even via email. Currently there is no standard way
to verify the authenticity of a stand-alone zone.

This document introduces a new RR type that serves as a cryptographic
message digest of the data in a zone. It allows a receiver of the
zone to verify the zone’s authenticity, especially when used in
combination with DNSSEC. This technique makes the message digest a
part of the zone itself, allowing verification the zone as a whole,
no matter how it is transmitted. Furthermore, the digest is based on
the wire format of zone data. Thus, it is independent of
presentation format, such as changes in whitespace, capitalization,
and comments.
DNSSEC provides three strong security guarantees relevant to this protocol:

1. whether or not to expect DNSSEC records in the zone,
2. whether or not to expect a ZONEMD record in a signed zone, and
3. whether or not the ZONEMD record has been altered since it was signed.

This specification is OPTIONAL to implement by both publishers and consumers of zone data.

1.1. Motivation

The motivation for this protocol enhancement is the desire for the ability to verify the authenticity of a stand-alone zone, regardless of how it is transmitted. A consumer of zone data should be able to verify that the data is as-published by the zone operator.

One approach to preventing data tampering and corruption is to secure the distribution channel. The DNS has a number of features that can already be used for channel security. Perhaps the most widely used is DNS transaction signatures (TSIG [RFC2845]). TSIG uses shared secret keys and a message digest to protect individual query and response messages. It is generally used to authenticate and validate UPDATE [RFC2136], AXFR [RFC5936], and IXFR [RFC1995] messages.

DNS Request and Transaction Signatures (SIG(0) [RFC2931]) is another protocol extension designed to authenticate individual DNS transactions. Whereas SIG records were originally designed to cover specific RR types, SIG(0) is used to sign an entire DNS message. Unlike TSIG, SIG(0) uses public key cryptography rather than shared secrets.

The Transport Layer Security protocol suite is also designed to provide channel security. One can easily imagine the distribution of zones over HTTPS-enabled web servers, as well as DNS-over-HTTPS [dns-over-https], and perhaps even a future version of DNS-over-TLS ([RFC7858]).

Unfortunately, the protections provided by these channel security techniques are (in practice) ephemeral and are not retained after the data transfer is complete. They can ensure that the client receives the data from the expected server, and that the data sent by the server is not modified during transmission. However, they do not guarantee that the server transmits the data as originally published, and do not provide any methods to verify data that is read after
transmission is complete. For example, a name server loading saved zone data upon restart cannot guarantee that the on-disk data has not been modified. For these reasons, it is preferable to secure the data itself.

Why not simply rely on DNSSEC, which provides certain data security guarantees? Certainly for zones that are signed, a recipient could validate all of the signed RRSets. Additionally, denial-of-existence records can prove that RRSets have not been added or removed. However, not all RRSets in a zone are signed. The design of DNSSEC stipulates that delegations (non-apex NS records) are not signed, and neither are any glue records. Thus, changes to delegation and glue records cannot be detected by DNSSEC alone. Furthermore, zones that employ NSEC3 with opt-out are susceptible to the removal or addition of names between the signed nodes. Whereas DNSSEC is primarily designed to protect consumers of DNS response messages, this protocol is designed to protect consumers of zones.

There are existing tools and protocols that provide data security, such as OpenPGP [RFC4880] and S/MIME [RFC3851]. In fact, the internic.net site publishes PGP signatures along side the root zone and other files available there. However, this is a detached signature with no strong association to the corresponding zone file other than its timestamp. Non-detached signatures are, of course, possible, but these necessarily change the format of the file being distributed. That is, a zone signed with OpenPGP or S/MIME no longer looks like a DNS zone and could not directly be loaded into a name server. Once loaded the signature data is lost, so it does not survive further propagation.

It seems the desire for data security in DNS zones was envisioned as far back as 1997. [RFC2065] is an obsoleted specification of the first generation DNSSEC Security Extensions. It describes a zone transfer signature, aka AXFR SIG, which is similar to the technique proposed by this document. That is, it proposes ordering all (signed) RRSets in a zone, hashing their contents, and then signing the zone hash. The AXFR SIG is described only for use during zone transfers. It did not postulate the need to validate zone data distributed outside of the DNS. Furthermore, its successor, [RFC2535], omits the AXFR SIG, while at the same time introducing an IXFR SIG.

1.2. Design Overview

This document introduces a new Resource Record type designed to convey a message digest of the content of a zone. The digest is calculated at the time of zone publication. Ideally the zone is signed with DNSSEC to guarantee that any modifications of the digest
can be detected. The procedures for digest calculation and DNSSEC signing are similar (i.e., both require the same ordering of RRs) and can be done in parallel.

The zone digest is designed to be used on zones that are relatively stable and have infrequent updates. As currently specified, the digest is re-calculated over the entire zone content each time. This specification does not provide an efficient mechanism for incremental updates of zone data. It does, however, reserve a field in the ZONEMD record for future work to support incremental zone digest algorithms (e.g. using Merkle trees).

It is expected that verification of a zone digest would be implemented in name server software. That is, a name server can verify the zone data it was given and refuse to serve a zone which fails verification. For signed zones, the name server needs a trust anchor to perform DNSSEC validation. For signed non-root zones, the name server may need to send queries to validate a chain-of-trust. Digest verification could also be performed externally.

1.3. Use Cases

1.3.1. Root Zone

The root zone [InterNIC] is one of the most widely distributed DNS zone on the Internet, served by 930 separate instances [RootServers] 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. [RFC7706] describes one, but not the only, way to do this. As the root zone spreads beyond its traditional deployment boundaries, the need for verification of the completeness of the zone contents becomes increasingly important.

1.3.2. Providers, Secondaries, and Anycast

Since its very early days, the developers of the DNS recognized the importance of secondary name servers and service diversity. However, they may not have anticipated the complexity of modern DNS service provisioning which can include multiple third-party providers and hundreds of anycast instances. Instead of a simple primary-to-secondary zone distribution system, today it is possible to have multiple levels, multiple parties, and multiple protocols involved in the distribution of zone data. This complexity introduces new places for problems to arise. The zone digest protects the integrity of data that flows through such systems.
1.3.3. Response Policy Zones

DNS Response Policy Zones is "a method of expressing DNS response policy information inside specially constructed DNS zones..." [RPZ]. A number of companies provide RPZ feeds, which can be consumed by name server and firewall products. Since these are zones, AXFR is often, but not necessarily used for transmission. While RPZ zones can certainly be signed with DNSSEC, the data is not queried directly, and would not be subject to DNSSEC validation.

1.3.4. Centralized Zone Data Service

ICANN operates the Centralized Zone Data Service [CZDS], which is a repository of top-level domain zone files. Users request access to the system, and to individual zones, and are then able to download zone data for certain uses. Adding a zone digest to these would provide CZDS users with assurances that the data has not been modified. Note that ZONEMD could be added to CZDS zone data independently of the zone served by production name servers.

1.3.5. General Purpose Comparison Check

Since the zone digest does not depend on presentation format, it could be used to compare multiple copies of a zone received from different sources, or copies generated by different processes.

1.4. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. The ZONEMD Resource Record

This section describes the ZONEMD Resource Record, including its fields, wire format, and presentation format. The Type value for the ZONEMD RR is 63. The ZONEMD RR is class independent. The RDATA of the resource record consists of four fields: Serial, Digest Type, Parameter, and Digest.

This specification utilizes ZONEMD RRs located at the zone apex. Non-apex ZONEMD RRs are not forbidden, but have no meaning in this specification.

A zone MAY contain multiple ZONEMD RRs to support algorithm agility [RFC7696] and rollovers. Each ZONEMD RR MUST specify a unique Digest
Type and Parameter tuple. It is RECOMMENDED that a zone include only
one ZONEMD RR, unless the zone publisher is in the process of
transitioning to a new Digest Type.

2.1. ZONEMD RDATA Wire Format

The ZONEMD RDATA wire format is encoded as follows:

```
+---+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             Serial                            |
+---+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Digest Type  |   Parameter   |                               |
+-----------------------------------+-----------------------------------|
|                             Digest                            |
+-----------------------------------+-----------------------------------|
/                               /                               /
/                               /                               /
+-----------------------------------------------------------------
```

2.1.1. The Serial Field

The Serial field is a 32-bit unsigned integer in network order. It
is equal to the serial number from the zone’s SOA record ([RFC1035]
section 3.3.13) for which the message digest was generated.

The zone’s serial number is included here in order to make DNS
response messages of type ZONEMD meaningful. Without the serial
number, a stand-alone ZONEMD digest has no association to any
particular instance of a zone.

2.1.2. The Digest Type Field

The Digest Type field is an 8-bit unsigned integer that identifies
the algorithm used to construct the digest.

At the time of this writing, SHA384-STABLE, with value 1, is the only
standardized Digest Type defined for ZONEMD records. The Digest Type
registry is further described in Section 6.

Digest Type values 240-254 are allocated for Private Use as described
in [RFC8126].

2.1.3. The Parameter Field

The Parameter field is an 8-bit unsigned integer whose meaning
depends on the Digest Type in use. For SHA384-STABLE, the Parameter
field plays no role in digest calculation or verification.
2.1.4. The Digest Field

The Digest field is a variable-length sequence of octets containing the message digest. The Digest field MUST NOT be empty. Section 3 describes how to calculate the digest for a zone. Section 4 describes how to use the digest to verify the contents of a zone.

2.2. ZONEMD Presentation Format

The presentation format of the RDATA portion is as follows:

The Serial field MUST be represented as an unsigned decimal integer.

The Digest Type field MUST be represented as an unsigned decimal integer.

The Parameter field MUST be represented as an unsigned decimal integer.

The Digest MUST be represented as a sequence of case-insensitive hexadecimal digits. Whitespace is allowed within the hexadecimal text.

2.3. ZONEMD Example

The following example shows a ZONEMD RR.

example.com. 86400 IN ZONEMD 2018031500 1 0 (FEBE3D4CE2EC2FFA4BA99D46CD69D6D29711E55217057BEE 7EB1A7B641A47BA7FED2DD5B97AE499FAFA4F22C6BD647DE )

3. Calculating the Digest

3.1. Canonical Format and Ordering

Calculation of the zone digest REQUIRES RRs to be processed in a consistent format and ordering. Correct ordering depends on (1) ordering of owner names, (2) ordering of RRs with the same owner name, and (3) ordering of RRs within an RRSet.

This specification adopts DNSSEC’s canonical ordering for names (Section 6.1 of [RFC4034]), and canonical ordering for RRs within an RRSet (Section 6.3 of [RFC4034]). It also adopts DNSSEC’s canonical RR form (Section 6.2 of [RFC4034]). However, since DNSSEC does not define a canonical ordering for RRSets having the same owner name, that ordering is defined here.
3.1.1. Order of RRSets Having the Same Owner Name

For the purposes of calculating the zone digest, RRSets having the same owner name MUST be numerically ordered, in ascending order, by their numeric RR TYPE.

3.1.2. Duplicate RRs

As stated in Section 5 of [RFC2181], it is meaningless for a zone to have multiple RRs with equal owner name, class, type, and RDATA. In the interest of consistency and interoperability, such duplicate RRs MUST NOT be included in the calculation of a zone digest.

3.2. Add ZONEMD Placeholder

In preparation for calculating the zone digest, any existing ZONEMD records at the zone apex MUST first be deleted.

Prior to calculation of the digest, and prior to signing with DNSSEC, a placeholder ZONEMD record MUST be added to the zone apex. This serves two purposes: (1) it allows the digest to cover the Serial, Digest Type, and Parameter field values, and (2) ensures that appropriate denial-of-existence (NSEC, NSEC3) records are created if the zone is signed with DNSSEC.

It is RECOMMENDED that the TTL of the ZONEMD record match the TTL of the SOA.

In the placeholder record, the Serial field MUST be set to the current SOA Serial. The Digest Type field MUST be set to the value for the chosen digest algorithm. The Parameter field is set to a value whose meaning depends on the Digest Type. The Digest field MUST be set to all zeroes and of length appropriate for the chosen digest algorithm.

If multiple digests are to be published in the zone, e.g., during an algorithm rollover, there MUST be one placeholder record for each Digest Type.

3.3. Optionally Sign the Zone

Following addition of placeholder records, the zone MAY be signed with DNSSEC. Note that when the digest calculation is complete, and the ZONEMD record is updated, the signature(s) for the ZONEMD RRSet MUST be recalculated and updated as well. Therefore, the signer is not required to calculate a signature over the placeholder record at this step in the process, but it is harmless to do so.
3.4. Calculate the Digest

The digest calculation details vary depending upon the Digest Type. This document describes digest calculation for SHA384-STABLE only. Digest calculation for additional types may be defined in future updates to this document.

3.4.1. SHA384-STABLE Calculation

The Parameter field is not used in the calculation of SHA384-STABLE message digests. The Parameter field SHOULD be set to zero in SHA384-STABLE placeholder records.

The zone digest is calculated by concatenating the canonical on-the-wire form (without name compression) of all RRs in the zone, in the order described above, subject to the inclusion/exclusion rules described below, and then applying the SHA384 digest algorithm [RFC6605]:

\[
\text{digest} = \text{SHA384}( \text{RR}(1) \ | \ \text{RR}(2) \ | \ \text{RR}(3) \ | \ ... )
\]

where "|" denotes concatenation, and

\[
\text{RR}(i) = \text{owner} \mid \text{type} \mid \text{class} \mid \text{TTL} \mid \text{RDATA length} \mid \text{RDATA}
\]

3.4.2. Inclusion/Exclusion Rules

When calculating the digest, the following inclusion/exclusion rules apply:

- All records in the zone, including glue records, MUST be included.
- Occluded data ([RFC5936] Section 3.5) MUST be included.
- Duplicate RRs with equal owner, class, type, and RDATA MUST NOT be included.
- The placeholder ZONEMD RR(s) MUST be included.
- If the zone is signed, DNSSEC RRs MUST be included, except:
- The RRSIG covering ZONEMD MUST NOT be included because the RRSIG will be updated after all digests have been calculated.
3.5. Update ZONEMD RR

Once a zone digest has been calculated, its value is then copied to the Digest field of the placeholder ZONEMD record. Repeat for each digest if multiple digests are to be published.

If the zone is signed with DNSSEC, the appropriate RRSIG records covering the ZONEMD RRSet MUST then be added or updated. Because the ZONEMD placeholder was added prior to signing, the zone will already have the appropriate denial-of-existence (NSEC, NSEC3) records.

Some implementations of incremental DNSSEC signing might update the zone’s serial number for each resigning. However, to preserve the calculated digest, generation of the ZONEMD signature at this time MUST NOT also result in a change of the SOA serial number.

4. Verifying Zone Message Digest

The recipient of a zone that has a message digest record can verify the zone by calculating the digest as follows:

1. The verifier SHOULD first determine whether or not to expect DNSSEC records in the zone. This can be done by examining locally configured trust anchors, or querying for (and validating) DS RRs in the parent zone. For zones that are provably insecure, digest validation continues at step 4 below.

2. For zones that are provably secure, the existence of the apex ZONEMD record MUST be verified. If the ZONEMD record provably does not exist, digest verification cannot be done. If the ZONEMD record does provably exist, but is not found in the zone, digest verification MUST NOT be considered successful.

3. For zones that are provably secure, the SOA and ZONEMD RRSets MUST have valid signatures, chaining up to a trust anchor. If DNSSEC validation of the SOA or ZONEMD records fails, digest verification MUST NOT be considered successful.

4. If the ZONEMD RRSet contains more than one RR with the same Digest Type and Parameter, digest verification MUST NOT be considered successful.

5. The SOA Serial field MUST exactly match the ZONEMD Serial field. If the fields do not match, digest verification MUST NOT be considered successful.

6. The ZONEMD Digest Type field MUST be checked. If the verifier does not support the given digest type, it SHOULD report that
the zone digest could not be verified due to an unsupported algorithm.

7. The received Digest Type and Digest values are copied to a temporary location.

8. The ZONEMD RR’s RDATA is reset to the placeholder values described in Section 3.2.

9. The zone digest is computed over the zone data as described in Section 3.4.

10. The calculated digest is compared to the received digest stored in the temporary location. If the two digest values match, verification is considered successful. Otherwise, verification MUST NOT be considered successful.

11. The ZONEMD RR’s RDATA is reset to the received Digest Type and Digest stored in the temporary location. Thus, any downstream clients can similarly verify the zone.

4.1. Verifying Multiple Digests

If multiple digests are present in the zone, e.g., during an algorithm rollover, a match using any one of the recipient’s supported Digest Type algorithms is sufficient to verify the zone.

5. Scope of Experimentation

This memo is published as an Experimental RFC. The purpose of the experimental period is to provide the community time to analyze and evaluate the methods defined in this document, particularly with regard to the wide variety of DNS zones in use on the Internet.

Additionally, the ZONEMD record defined in this document includes a Parameter field in the form of an 8-bit integer. The authors have a particular future use in mind for this field, namely to support efficient digests in large, dynamic zones. We intend to conduct future experiments using Merkle trees of varying depth. The choice of tree depth can be encoded in this reserved field. We expect values for tree depth to range from 0 to 10, requiring at most four bits of this field. This leaves another four bits available for other future uses, if absolutely necessary.

The duration of the experiment is expected to be no less than two years from the publication of this document. If the experiment is successful, it is expected that the findings of the experiment will result in an updated document for Standards Track approval.
6. IANA Considerations

6.1. ZONEMD RRtype

This document defines a new DNS RR type, ZONEMD, whose value 63 has been allocated by IANA from the "Resource Record (RR) TYPEs" subregistry of the "Domain Name System (DNS) Parameters" registry:

Type: ZONEMD

Value: 63

Meaning: Message Digest Over Zone Data

Reference: This document

6.2. ZONEMD Digest Type

This document asks IANA to create a new "ZONEMD Digest Types" registry with initial contents as follows:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Mnemonic</th>
<th>Status</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SHA384 for stable zones</td>
<td>SHA384-STABLE</td>
<td>Mandatory</td>
<td>This document</td>
</tr>
<tr>
<td>240-254</td>
<td>Private Use</td>
<td>-</td>
<td>-</td>
<td>[RFC8126]</td>
</tr>
</tbody>
</table>

Table 1: ZONEMD Digest Types

7. Security Considerations

7.1. Attacks Against the Zone Digest

The zone digest allows the receiver to verify that the zone contents haven’t been modified since the zone was generated/published. Verification is strongest when the zone is also signed with DNSSEC. An attacker, whose goal is to modify zone content before it is used by the victim, may consider a number of different approaches.

The attacker might perform a downgrade attack to an unsigned zone. This is why Section 4 RECOMMENDS that the verifier determine whether or not to expect DNSSEC signatures for the zone in step 1.

The attacker might perform a downgrade attack by removing the ZONEMD record. This is why Section 4 REQUIRES that the verifier checks DNSSEC denial-of-existence proofs in step 2.
The attacker might alter the Digest Type or Digest fields of the ZONEMD record. Such modifications are detectable only with DNSSEC validation.

7.2. Attacks Utilizing the Zone Digest

Nothing in this specification prevents clients from making, and servers from responding to, ZONEMD queries. One might consider how well ZONEMD responses could be used in a distributed denial-of-service amplification attack.

The ZONEMD RR is moderately sized, much like the DS RR. A single ZONEMD RR contributes approximately 40 to 65 octets to a DNS response, for currently defined digest types. Certainly other query types result in larger amplification effects (i.e., DNSKEY).

8. Privacy Considerations

This specification has no impacts on user privacy.

9. Acknowledgments

The authors wish to thank David Blacka, Scott Hollenbeck, and Rick Wilhelm for providing feedback on early drafts of this document. Additionally, they thank Joe Abley, Mark Andrews, Ralph Dolmans, Richard Gibson, Olafur Gudmundsson, Paul Hoffman, Evan Hunt, Shumon Huque, Tatuya Jinmei, Burt Kaliski, Shane Kerr, Matt Larson, John Levine, Ed Lewis, Matt Pounsett, Mukund Sivaraman, Petr Spacek, Ondrej Sury, Willem Toorop, Florian Weimer, Tim Wicinski, Wouter Wijngarrds, Paul Wouters, and other members of the dnsop working group for their input.

10. Implementation Status

10.1. Authors’ Implementation

The authors have an open source implementation in C, using the ldns library [ldns-zone-digest]. This implementation is able to perform the following functions:

- Read an input zone and output a zone with the ZONEMD placeholder.
- Compute zone digest over signed zone and update the ZONEMD record.
- Re-compute DNSSEC signature over the ZONEMD record.
- Verify the zone digest from an input zone.
This implementation does not:

- Perform DNSSEC validation of the ZONEMD record during verification.

### 10.2. Shane Kerr’s Implementation

Shane Kerr wrote an implementation of this specification during the IETF 102 hackathon [ZoneDigestHackathon]. This implementation is in Python and is able to perform the following functions:

- Read an input zone and an output zone with ZONEMD record.
- Verify the zone digest from an input zone.
- Output the ZONEMD record in its defined presentation format.

This implementation does not:

- Re-compute DNSSEC signature over the ZONEMD record.
- Perform DNSSEC validation of the ZONEMD record.

### 11. Change Log

RFC Editor: Please remove this section.

This section lists substantial changes to the document as it is being worked on.

From -00 to -01:

- Removed requirement to sort by RR CLASS.
- Added Kumari and Hardaker as coauthors.
- Added Change Log section.
- Minor clarifications and grammatical edits.

From -01 to -02:

- Emphasize desire for data security over channel security.
- Expanded motivation into its own subsection.
- Removed discussion topic whether or not to include serial in ZONEMD.
Clarified that a zone’s NS records always sort before the SOA record.

Clarified that all records in the zone must be digested, except as specified in the exclusion rules.

Added for discussion out-of-zone and occluded records.

Clarified that update of ZONEMD signature must not cause a serial number change.

Added persons to acknowledgments.

From -02 to -03:

Added recommendation to set ZONEMD TTL to SOA TTL.

Clarified that digest input uses uncompressed names.

Updated Implementations section.

Changed intended status from Standards Track to Experimental and added Scope of Experiment section.

Updated Motivation, Introduction, and Design Overview sections in response to working group discussion.

Gave ZONEMD digest types their own status, separate from DS digest types. Request IANA to create a registry.

Added Reserved field for future work supporting dynamic updates.

Be more rigorous about having just ONE ZONEMD record in the zone.

Expanded use cases.

From -03 to -04:

Added an appendix with example zones and digests.

Clarified that only apex ZONEMD RRs shall be processed.

From -04 to -05:

Made SHA384 the only supported ZONEMD digest type.

Disassociated ZONEMD digest types from DS digest types.
o Updates to Introduction based on list feedback.

o Changed "zone file" to "zone" everywhere.

o Restored text about why ZONEMD has a Serial field.

o Clarified ordering of RRSets having same owner to be numerically ascending.

o Clarified that all duplicate RRs (not just SOA) must be suppressed in digest calculation.

o Clarified that the Reserved field must be set to zero and checked for zero in verification.

o Clarified that occluded data must be included.

o Clarified procedure for verification, using temporary location for received digest.

o Explained why Reserved field is 8-bits.

o IANA Considerations section now more specific.

o Added complex zone to examples.

From -05 to -06:

o RR type code 63 was assigned to ZONEMD by IANA.

From -06 to -07:

o Fixed mistakes in ZONEMD examples.

o Added private use Digest Type values 240-254.

o Clarified that Digest field must not be empty.

From -07 to draft-ietf-dnsop-dns-zone-digest-00:

o Adopted by dnsop.

o Clarified further that non-apex ZONEMD RRs have no meaning.

o Changed "provably [un]signed" to "provably [in]secure".
o Allow multiple ZONEMD RRs to support algorithm agility/rollovers.

o Describe verification when there are multiple ZONEMD RRs.

From -00 to -01:

- Simplified requirements around verifying multiple digests. Any one match is sufficient.
- Updated implementation notes.
- Both implementations produce expected results on examples given in this document.

From -01 to -02:

- Changed the name of the Reserved field to Parameter.
- Changed the name of Digest Type 1 from SHA384 to SHA384-STABLE.
- The meaning of the Parameter field now depends on Digest Type.
- No longer require Parameter field to be zero in verification.
- Updated a rule from earlier versions that said multiple ZONEMD RRs were not allowed.

12. References

12.1. Normative References


12.2.  Informative References


Internet-Draft               DNS Zone Digest                October 2019

[RFC2535] Eastlake 3rd, D., "Domain Name System Security
Extensions", RFC 2535, DOI 10.17487/RFC2535, March 1999,

[RFC2845] Vixie, P., Gudmundsson, O., Eastlake 3rd, D., and B.
Wellington, "Secret Key Transaction Authentication for DNS
(TSIG)", RFC 2845, DOI 10.17487/RFC2845, May 2000,

[RFC2931] Eastlake 3rd, D., "DNS Request and Transaction Signatures
(SIG(0)s)", RFC 2931, DOI 10.17487/RFC2931, September

[RFC3851] Ramsdell, B., Ed., "Secure/Multipurpose Internet Mail
Extensions (S/MIME) Version 3.1 Message Specification",
RFC 3851, DOI 10.17487/RFC3851, July 2004,

Thayer, "OpenPGP Message Format", RFC 4880,
DOI 10.17487/RFC4880, November 2007,

(AXFR)", RFC 5936, DOI 10.17487/RFC5936, June 2010,

[RFC7696] Housley, R., "Guidelines for Cryptographic Algorithm
Agility and Selecting Mandatory-to-Implement Algorithms",
BCP 201, RFC 7696, DOI 10.17487/RFC7696, November 2015,

Servers by Running One on Loopback", RFC 7706,
DOI 10.17487/RFC7706, November 2015,

Terminology", RFC 7719, DOI 10.17487/RFC7719, December

and P. Hoffman, "Specification for DNS over Transport
Appendix A. Example Zones With Digests

This appendix contains example zones with accurate ZONEMD records. These can be used to verify an implementation of the zone digest protocol.

A.1. Simple EXAMPLE Zone

Here, the EXAMPLE zone contains an SOA record, NS and glue records, and a ZONEMD record.

```plaintext
example. 86400 IN SOA ns1 admin 2018031900 ( 1800 900 604800 86400 )
          86400 IN NS ns1
          86400 IN NS ns2
          86400 IN ZONEMD 2018031900 1 0 ( 379ec2587d4fff35 0062b9385a641476 6f9c028e8cf09d8a 7965537a68a2f149 4e1c151f8cf6be05 5bef4f27e6a87b13 )
ns1 3600 IN A 127.0.0.1
ns2 3600 IN AAAA ::1
```
A.2. Complex EXAMPLE Zone

Here, the EXAMPLE zone contains duplicate RRs, and an occluded RR, and one out-of-zone RR.

```plaintext
example.      86400   IN  SOA     ns1 admin 2018031900 (  
              1800 900 604800 86400 )
86400   IN  NS      ns1
86400   IN  NS      ns2
86400   IN  ZONEMD  2018031900 1 0 (  
              c36e77eafdb7f3f6  
              dcfac8bca1121e17  
              2a7b57db2c88409a  
              5c3d9247ba72b759  
              6c735c1a76fc817a  
              ad5c834f5a4bce16 )
ns1           3600    IN  A       127.0.0.1
ns2           3600    IN  AAAA    ::1
occluded.sub  7200    IN  TXT     "I’m occluded but must be digested"
sub           7200    IN  NS      ns1
duplicate     300     IN  TXT     "I must be digested just once"
duplicate     300     IN  TXT     "I must be digested just once"
foo.test.     555     IN  TXT     "out-of-zone data must be excluded"
on-apex       900     IN  ZONEMD  2018031900 1 0 (  
              616c6c6f77656420  
              6275742069676e6f  
              7265642e20616c6c  
              6f77656420627574  
              2069676e6f726564  
              2e20616c6f7765 )
```

A.3. EXAMPLE Zone with multiple digests

Here, the EXAMPLE zone contains multiple ZONEMD records. Since only one Digest Type is defined at this time (SHA384-STABLE), this example utilizes additional ZONEMD records with Digest Type values in the private range (240-254). These additional private-range digests are not verifiable, but note that their other fields (Serial, Parameter, Digest Type) are included in the calculation of all ZONEMD digests.
example. 86400 IN SOA ns1 admin 2018031900 (1800 900 604800 86400 )
example. 86400 IN NS ns1.example.
example. 86400 IN NS ns2.example.
example. 86400 IN ZONEMD 2018031900 1 0 (c0218e8e6b4f0275d54c0e577e91f4d23742b4756708d50d712114d34b99a8f869e0b071a2b02750457c87870bc8c0d2)
example. 86400 IN ZONEMD 2018031900 240 0 (e2d523f654b9422a96c5a2f4f6670bbee)
example. 86400 IN ZONEMD 2018031900 241 0 (5732dd91246061f831a6b64769b3d2)
example. 86400 IN ZONEMD 2018031900 242 0 (7c32e06779315c7d81b87c72f5cf9116496b6395)
example. 86400 IN ZONEMD 2018031900 243 0 (183770af4e629f802e674e305b8d6d13dfe0837)
example. 86400 IN ZONEMD 2018031900 244 0 (e1846540e33a9e4189792d1835d131f605fc283e)
ns1.example. 3600 IN A 127.0.0.1
ns2.example. 86400 IN TXT "This example has multiple digests"
ns2.example. 3600 IN AAAA ::1

A.4. The URI.ARPA Zone

The URI.ARPA zone retrieved 2018-10-21.

; <<< DiG 9.9.4 <<< @lax.xfr.dns.icann.org uri.arpa axfr
; (2 servers found)
;; global options: +cmd
uri.arpa. 3600 IN SOA sns.dns.icann.org. (noc.dns.icann.org. 2018100702 10800 3600 1209600 3600 )
uri.arpa. 3600 IN RRSIG NSEC 8 2 3600 (e12018028142623 20181007205525 47155 uri.arpa.
eEC4w/oXLR1Epwgv4MB1dTSBxHqrJvW/UpbX8XpetAvD35bxwNCUTi/pAJVUXefgWeiriD2rkTgC8CMn7YQIIm3gdR+HjY/+o3BXNQzn97f+e
HAE9EDDzoNVfL1PyV/2fde9tDeUuAGVvWmD399NQg9jWytMryl2kysr q/g= )
uri.arpa. 86400 IN RRSIG NS 8 2 86400 (}
20181028172020 20181007175821 47155 uri.arpa.
ATyV2A2A8zogGC+8u4GuIP5MOuRu+3rr3eW0KEU55zAHid/7/FiBx141n
4byjY7?NudwUlM0EXaqjFZ/E7yV18PcvpP3HeeGavzQwawj+aus0jbfK
Bsvs2b1q2ZemBfkz/1fAhvUJkntoV5u1cJoKf1tu0GjyYNJcz2CqEuGD Wxc= )

url.arpa. 600 IN RRSIG MX 8 2 600 ( 20181028170556 20181007175821 47155 uri.arpa.
e7/r3KXDohX1lyVavetFF0bpb8B8aXT61hN9kCQD5xSnhgNM3UQVoT
1TtD8JVeINmCvCFNZp2pqgw1gB7xHtTm6Buer/m5E5+4uSnVeS6Q66H8ZK
A3mR95IpevuVIzvvVj+GcCAQpBo6kRODyVj/c/ZG6sfYWk7z7q/Em5/+ 3UI= )

url.arpa. 3600 IN RRSIG DNSSKEY 8 2 3600 ( 20181028152832 20181007175821 55480 uri.arpa.
nzpbhno0QsQgdB88z7tG7vP3wAYOdBUuw1l+rtjW1WYiqjpxZ286
XF4Rqlusf5Vx71j2z51Gsw+oaQqia9ylodFpLuXD6FTGm2nXGhN KKv1G
chHgtwj70XU72GefVg087xxyFzxxUFEP5ZTP9279FVWVVyyF86sbBr
6DZj3uIAw2eqBVLECgJlrMq99y7MueJ13UA4hE462O2J9Y9p0W9woqOB
dqkkwTWzogyYffmGAJG91RJ2h6cHtFJeZezMnay2glqi9Z0WT9VxXxd
uFPm0KD9U77A+ZtcAf9tsZwSdAoL365E2L1usZbaA+K0BnPpGFJRJk
5ROa1w= )

url.arpa. 3600 IN RRSIG DNSSKEY 8 2 3600 ( 20181028152832 20181007175821 55480 uri.arpa.
1WtQV/5qzoQjkXmbcd47/+COW8kJPKsRFlHxmxmt906+DByfhr6uq5X
nHvrvU1Q06M2uhqDeL+bDFVqgSpNvY+42/OaZvaK3j8EzPZPVBRPYkKMV
63T83aAIrAyHzoEdmzLCpalqcEE2ImzlHlsafManRfJL8yuv+JZDFj
2WDFfEcuUwkmIZW11xzp+DwxyUL1R17x+4ok5IKZW1gSUnBaf6BT75
WnxZihXwF3FzpXl0a51Yg71L3Tpx/xhJN6y9jGLIRF5BjIS9Xzrz3a2R
PkJ1095SnuEwHyp1mDAMv5BmQrLGrownjyvXAH7ho2m+mv4S8P5dUdxF+GTeA
1HeBfw= )

url.arpa. 3600 IN RRSIG SOA 8 2 3600 ( 20181029114753 20181008222815 47155 uri.arpa.
qn8yBNoHDjd7902wu9ItahoSOYPogp81G+qwPCRZBwGiHywuoUa2
Mx6BWZlg+HDyaj2j1Omox+IIqoUHhUOBo7IUKJf1grOKb9R2t8ThxR
9BUXqy95coV16wYm3BkTEPPxynX5Ffmy8vcndnKAF7sxSY8BbaYnPRejdx4A JUc= )

url.arpa. 3600 IN NSEC ftp.uri.arpa. NS SOA ( 20181028152832 20181007175821 55480 uri.arpa.
x.a.iana-servers.net.
url.arpa. 86400 IN NS a.iana-servers.net.
url.arpa. 86400 IN NS b.iana-servers.net.
url.arpa. 86400 IN NS c.iana-servers.net.
url.arpa. 86400 IN NS ns2.lacnic.net.
url.arpa. 86400 IN NS sec3.apnic.net.
url.arpa. 600 IN MX 10 pechora.icann.org.
url.arpa. 3600 IN DNSSKEY 256 3 8 ( 20181029114753 20181008222815 47155 uri.arpa.
AwEAAcBi7tSart2j599zbyWVspMNGN70IBW4ziqyQY9MTB/VCz6wYUK
uXunwllJbbQ3bcLqTlWEw134B6cTMHrZpJTab5WAwg4XCWUu8m0dcPTiL
B16qVRlR0WDwFPTzuYUKwsh1Brr7rvr5QbF5rh71zSpw5Vjjp65Wx
SdJj1H0B )

url.arpa. 3600 IN DNSSKEY 257 3 8 ( 20181028152832 20181007175821 55480 uri.arpa.
AwEAAAbNVv6ulGu8D31MtAehz7j3ALRjwZgv1WeszvN1Q1/+hBRZ9QyO
co2I+Dk0Q41NKox4D0UlXj8SxPO3wDuOF89q2/CF1200mZjafbdlytWc

3zSdBbi3q0cwCIx7GuG9eqll+pg7mdk9dgNZfhwB0LqTdD8ebLPsro/
Id7kBaiqYOQlZnX2Fzp+2h60j2HTy0DK1UssyB5PKsE0tvz0s6z9
IXKe5u+8WtMAgDY4tvG80JPAK7ezMih/NZcUMlE0PR28d3fog2duS5
ym+vA8327v8A+Rwh4UGjnxB8zmr803VOASAmHz/gwH5VbOnIiOObwFt
13wpBpr+wpm=)
uri.arpa. 3600 IN DNSKEY 257 3 8 (AwEAAbwnFTakCvaUXj4mgmxZUJ11ybgmGahbkmFEa0L16J+TchKR
wcqzVf3xUGa2MmeA4hkgAooC3uy+tTmoMsay8uq/JAj243jh2z46L5FD
FK/qMiDvQepYSHeq2vSv0jkuIsx4e4KsaFWYNOczKzG51oGjN2aJG
mrmI++xChpOsgkCsQY165mizUzfzjxJx1Auts+ecAiIvEqRaQfr8LRU
7WlsLximXirprtQrborzEtvl1hp9QXE6ART7QzfjjsNpKvFzmxZzF3
es/UJz5eHjwpDSIL7x8e1e01nGftJx9zN3b3bap1taJ5wY+5XOCkgy0
xmJUVNQwdE=)
ftp.uri.arpa. 3600 IN RRSIG NSEC 8 3 604800
(2018020800856 20180107175821 47155 uri.arpa.
HC1GqFpxzkYAT7Q/QntQeB6yrkPEPofe+9Q05/2zngwAewXEAQiyF9
jD1USjroMll1QbS3va3idW/LXoRs4E3hlCkn01cKHSuWaqzmE+BPP
Arfh8N95jgh/q6vpaB9utMkG3ttM2fyU1Gsz0NL0knxbHDHAv2axsMGH
1qM=)
ftp.uri.arpa. 604800 IN RRSIG NAPTR 8 3 604800
(201802103644 20180107205525 47155 uri.arpa.
WoLi+vZxoaLrz2IGznwrbVcf6kx1Wqd4WZP/U+AWnV+7MigsWP2af0
9toRereroGFiOoASXj2J6CJRmgmavOM9U+LZSconP9znNF4du6k5p
Yx1Qj0uH0vx1ZHFcj6lAt1ACUiw04Zm7MzEOMepvn?iH7r7 k7k=
)
ftp.uri.arpa. 3600 IN NSEC http://uri.arpa. NAPTR (RRSIG NSEC)
ftp.uri.arpa. 604800 IN NAPTR 0 0 "" "" (""ftp://{[^:/?#]*}.*$!\1!i"")
http.uri.arpa. 3600 IN RRSIG NSEC 8 3 604800
(2018020910647 20180107175821 47155 uri.arpa.
U03Nh7Q73LHwPflMUK8mMsqkwVsOGw2KdsyHyAjqQ8SzvKbtmbv7HBmE
H1+i13Z+wtf2Mg5y5ac/6shdx69bfJzs16xumyMc1AgY6325KDTQbIMN+
ift9GrBC7CgCd2msf/uzSrYxxg4MQJqBFpvlkxYn3b7eJ51lX1sBIn7
3b8=)
http.uri.arpa. 604800 IN RRSIG NAPTR 8 3 604800
(2018020911815 20180107205525 47155 uri.arpa.
T7mrRdrag+sMg+223mBTQ/Y3v+rdDnFvQ90LN5Fq32NK21fYajF7F
Tp560ouynfL4fIhroE0wrc9NwoCUC0uc9C7Wai1jQc1elvagoAM+L6f0
RsEjQw6+9jv1LrMKQvXoQ0mxLV17338uoD/xiAFOsSnDbiQxWmQVAimv5
7Zs=)
http.uri.arpa. 3600 IN NSEC mailto.uri.arpa. NAPTR (RRSIG NSEC)
http.uri.arpa. 604800 IN NAPTR 0 0 "" "" (""mailto://{[^:/?#]*}.*$!\1!i"")
mailto.uri.arpa. 3600 IN RRSIG NSEC 8 3 604800
(20180110727 20180107175821 47155 uri.arpa.
GvxzVL85rEukwGqtuLxek9wjpwBMFt0FIeYj7afC8HxVMs6mFa/nEM/
IdFrVfG+1YoJSQYuSAYYP13xPbgxVSLL125qtfCMdC/YjuZEng51c
fQciMRD7R3+znZf8m8d8u/snLV5w4D+1TBzRjJUBe1Ef6c6=8vumV7V819
Zoy=)
mailto.uri.arpa. 604800 IN RRSIG NAPTR 8 3 604800
(201802124825 20180107205525 47155 uri.arpa.)
A.5. The ROOT-SERVERS.NET Zone

The ROOT-SERVERS.NET zone retrieved 2018-10-21.
Authors’ Addresses

Duane Wessels
Verisign
12061 Bluemont Way
Reston, VA 20190

Phone: +1 703 948-3200
Email: dwessels@verisign.com
URI: http://verisign.com

Piet Barber
Verisign
12061 Bluemont Way
Reston, VA 20190

Phone: +1 703 948-3200
Email: pbarber@verisign.com
URI: http://verisign.com

Matt Weinberg
Verisign
12061 Bluemont Way
Reston, VA 20190

Phone: +1 703 948-3200
Email: mweinberg@verisign.com
URI: http://verisign.com

Warren Kumari
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043

Email: warren@kumari.net

Wes Hardaker
USC/ISI
P.O. Box 382
Davis, CA 95617

Email: ietf@hardakers.net