dnsop
Internet-Draft
Intended status: Standards Track
Expires: 11 February 2022

P. van Dijk
PowerDNS

10 August 2021

The VERBATIM Digest Algorithm for DS records
draft-vandijk-dnsop-ds-digest-verbatim-01

Abstract

The VERBATIM DS Digest is defined as a direct copy of the input data without any hashing.

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."

This Internet-Draft will expire on 11 February 2022.

Copyright Notice

Table of Contents

1. Introduction

The currently defined DS Digest Algorithms take the input data and hash it into a fixed-length form using well defined hashing algorithms (several SHA variants, and one mostly unused GOST algorithm). That hashing operation makes any data inside the (C)DNSKEY record unreachable until that data is retrieved from the child zone. Thus, DS records do not actually convey information; they merely verify information that can be retrieved elsewhere.

A DS record set can only answer the question 'this data that I have here, do you recognise it?'. In that sense, DS records are not information sources - they are boolean oracles. For several imagined use cases for signed data at the parent, this might not be sufficient. One such use case is https://datatracker.ietf.org/doc/draft-schwartz-ds-glue/ (https://datatracker.ietf.org/doc/draft-schwartz-ds-glue/) [FIXME: make this a proper ref].

This document introduces a new Digest Algorithm, proposed name VERBATIM (alternative suggestion: NULL). The VERBATIM Digest Algorithm takes the input data (DNSKEY owner name | DNSKEY RDATA per section 5.1.4 of [RFC4034]) and copies it unmodified into the DS Digest field.

2. Document work

This document lives on GitHub (https://github.com/PowerDNS/draft-dnsop-ds-digest-verbatim); proposed text and editorial changes are very much welcomed there, but any functional changes should always first be discussed on the IETF DNSOP WG mailing list.

3. Conventions and Definitions

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.

4. Implementation

The subsection titles in this section attempt to follow the terminology from [RFC8499] in as far as it has suitable terms. 'Implementation' is understood to mean both 'code changes' and 'operational changes' here.

4.1. Authoritative server changes

None, except where related tooling emits DS records to the administrator.

4.2. Validating resolver changes

Validating resolvers are encouraged to implement the VERBATIM Digest Algorithm.

4.3. Stub resolver changes

This specification defines no changes to query processing in stub resolvers.

4.4. Zone validator changes

Zone validators are encouraged to recognise the VERBATIM Digest Algorithm and, where possible, verify it against the child zone's DNSKEY, if it has any for the given algorithm.

4.5. Domain registry changes

Domain registries are encouraged to allow VERBATIM digests at their user's request. However, a likely outcome is that domain registries will only allow the VERBATIM digest for DNSSEC algorithms whose specifications call for use of the VERBATIM digest.

5. Security Considerations

Previously existing DS Digest Algorithms have a fixed size output. The VERBATIM digest has a variable size output, that may be under the control of a third party, like the owner of a delegated domain. Such a third party might cause zone files to grow very big with just a few data submissions to a registrar/registry. DNS query responses containing VERBATIM digests might also be bigger than is desired.

Implementors, specifically domain registries, may want to limit use of VERBATIM to specified use cases, and with limits appropriate to those use cases.

6. Implementation Status

[RFC Editor: please remove this section before publication]

7. IANA Considerations

This document updates the IANA registry "Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms" at https://www.iana.org/assignments/ds-rr-types/ds-rr-types.xhtml

(https://www.iana.org/assignments/ds-rr-types/ds-rr-types.xhtml)

The following entry is added to the registry:

Value	TBD
Description	VERBATIM
Status	OPTIONAL
Reference	RFC TBD2

8. Acknowledgements

9. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <https://www.rfc-editor.org/info/rfc4034>.

10. Informative References

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

Appendix A. Document history

Author's Address

Peter van Dijk
PowerDNS
Den Haag

Netherlands

Email: peter.van.dijk@powerdns.com