Network Working Group
Internet-Draft
Updates: 4034, 5155 (if approved)
Intended status: Standards Track
Expires: 14 March 2026

W. Hardaker
USC/ISI
W. Kumari
Google

10 September 2025

Deprecating the use of SHA-1 in DNSSEC signature algorithms
draft-ietf-dnsop-must-not-sha1-10

Abstract

This document deprecates the use of the RSASHA1 and RSASHA1-NSEC3-SHA1 algorithms for the creation of DNS Public Key (DNSKEY) and Resource Record Signature (RRSIG) records.

It updates RFC4034 and RFC5155 as it deprecates the use of these algorithms.

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 14 March 2026.

Copyright Notice

Table of Contents

1. Introduction

The security of the protection provided by the SHA-1 algorithm [RFC3174] has been slowly diminishing over time as various forms of attacks have weakened its cryptographic underpinning. DNSSEC [RFC9364] originally [RFC3110] made extensive use of SHA-1, for example as a cryptographic hash algorithm in RRSIG and Delegation Signer (DS) records. Since then, multiple other algorithms with stronger cryptographic strength have become widely available for DS records and for Resource Record Signature (DNSKEY) and DNS Public Key (RRSIG) records [RFC4034]. Operators are encouraged to consider switching to one of the recommended algorithms listed in the [DNSKEY-IANA] and [DS-IANA] tables, respectively. Further, support for validating SHA-1 based signatures has been removed from some systems. As a result, SHA-1 as part of a signature algorithm is no longer fully interoperable in the context of DNSSEC. As adequate alternatives exist, the use of SHA-1 is no longer advisable.

This document thus further deprecates the use of RSASHA1 and RSASHA1-NSEC3-SHA1 for DNS Security Algorithms.

1.1. Requirements notation

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. Deprecating SHA-1 from DNSSEC Signatures and Delegation RRs

The RSASHA1 [RFC4034] and RSASHA1-NSEC3-SHA1 [RFC5155] algorithms MUST NOT be used when creating DS records. Operators of validating resolvers MUST treat RSASHA1 and RSASHA1-NSEC3-SHA1 DS records as insecure. If no other DS records of accepted cryptographic algorithms are available, the DNS records below the delegation point MUST be treated as insecure.

The RSASHA1 [RFC4034] and RSASHA1-NSEC3-SHA1 [RFC5155] algorithms MUST NOT be used when creating DNSKEY and RRSIG records. Validating resolver implementations ([RFC9499] section 10) MUST continue to support validation using these algorithms as they are diminishing in use but still actively in use for some domains as of this publication. Operators of validating resolvers MUST treat DNSSEC signing algorithms RSASHA1 and RSASHA1-NSEC3-SHA1 as unsupported, rendering responses insecure if they cannot be validated by other supported signing algorithms.

3. Security Considerations

This document deprecates the use of RSASHA1 and RSASHA1-NSEC3-SHA1 for DNSSEC Delegation and DNSSEC signing since these algorithms are no longer considered to be secure.

4. Operational Considerations

Zone owners currently making use of SHA-1 based algorithms should immediately roll to algorithms with stronger cryptographic algorithms, such as the recommended algorithms in the [DNSKEY-IANA] and [DS-IANA] tables.

Operators should take care when deploying software packages and operating systems that may have already removed support for the SHA-1 algorithm. In these situations software may need to be manually built and deployed by an operator to continue supporting the required levels indicated by the "Use for DNSSEC Validation" and "Implement for DNSSEC Validation" columns, which this document is not changing.

5. IANA Considerations

[Note to IANA, to be removed by the RFC Editor: the registry fields listed above will be created by draft-ietf-dnsop-rfc8624-bis.]

IANA is requested to set the "Use for DNSSEC Delegation" field of the "Digest Algorithms" registry [DS-IANA] [I-D.ietf-dnsop-rfc8624-bis] for SHA-1 (1) to MUST NOT.

IANA is requested to set the "Use for DNSSEC Signing" column of the DNS Security Algorithm Numbers registry [DNSKEY-IANA] [I-D.ietf-dnsop-rfc8624-bis] to MUST NOT for the RSASHA1 (5) and RSASHA1-NSEC3-SHA1 (7) algorithms.

All other columns should remain as currently specified.

6. Normative References

[DNSKEY-IANA] IANA, "Domain Name System Security (DNSSEC) Algorithm Numbers", n.d., <https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml>.

[DS-IANA] IANA, "Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms", n.d., <http://www.iana.org/assignments/ds-rr-types>.

[I-D.ietf-dnsop-rfc8624-bis] Hardaker, W. and W. Kumari, "DNSSEC Cryptographic Algorithm Recommendation Update Process", Work in Progress, Internet-Draft, draft-ietf-dnsop-rfc8624-bis-13, 4 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-rfc8624-bis-13>.

[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/rfc/rfc2119>.

[RFC3110] Eastlake 3rd, D., "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)", RFC 3110, DOI 10.17487/RFC3110, May 2001, <https://www.rfc-editor.org/rfc/rfc3110>.

[RFC3174] Eastlake 3rd, D. and P. Jones, "US Secure Hash Algorithm 1 (SHA1)", RFC 3174, DOI 10.17487/RFC3174, September 2001, <https://www.rfc-editor.org/rfc/rfc3174>.

[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/rfc/rfc4034>.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, DOI 10.17487/RFC5155, March 2008, <https://www.rfc-editor.org/rfc/rfc5155>.

[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/rfc/rfc8174>.

[RFC9364] Hoffman, P., "DNS Security Extensions (DNSSEC)", BCP 237, RFC 9364, DOI 10.17487/RFC9364, February 2023, <https://www.rfc-editor.org/rfc/rfc9364>.

[RFC9499] Hoffman, P. and K. Fujiwara, "DNS Terminology", BCP 219, RFC 9499, DOI 10.17487/RFC9499, March 2024, <https://www.rfc-editor.org/rfc/rfc9499>.

Appendix A. Acknowledgments

The authors appreciate the comments and suggestions from the following IETF participants in helping produce this document: Mark Andrews, Steve Crocker, Peter Dickson, Thomas Graf, Paul Hoffman, Russ Housley, Shumon Huque, Barry Leiba, S Moonesamy, Yoav Nir, Florian Obser, Peter Thomassen, Stefan Ubbink, Paul Wouters, Tim Wicinski, and the many members of the DNSOP working group that discussed this draft.

Appendix B. Current algorithm usage levels

The DNSSEC scanning project by Viktor Dukhovni and Wes Hardaker highlights the current deployment of various algorithms on the https://stats.dnssec-tools.org/ website.

<RFC Editor: please delete this section upon publication>

Appendix C. Github Version of this document

While this document is under development, it can be viewed, tracked, fill here:

https://github.com/hardaker/draft-hardaker-dnsop-must-not-sha1

<RFC Editor: please delete this section upon publication>

Authors' Addresses

Wes Hardaker
USC/ISI
Email: ietf@hardakers.net

Warren Kumari
Google
Email: warren@kumari.net