Stream:	Internet Engineering Task Force (IETF)
RFC:	9905
Updates:	4034, 5155
Category:	Standards Track
Published:	October 2025
ISSN:	2070-1721
Authors:	W. Hardaker	W. Kumari
---	---	---
	USC/ISI	*Google*

RFC 9905
Deprecating the Use of SHA-1 in DNSSEC Signature Algorithms

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 RFCs 4034 and 5155 as it deprecates the use of these algorithms.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9905.

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 defined in [RFC3110]) made extensive use of SHA-1, for example, as a cryptographic hash algorithm in Resource Record Signature (RRSIG) and Delegation Signer (DS) records. Since then, multiple other algorithms with stronger cryptographic strength have become widely available for DS records and for RRSIG and DNS Public Key (DNSKEY) records [RFC4034]. Operators are encouraged to consider switching to one of the recommended algorithms listed in the "DNS Security Algorithm Numbers" [DNSKEY-IANA] and "DNS Security Algorithm Numbers" [DS-IANA] registries, 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 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 switch to algorithms with stronger cryptographic algorithms, such as the recommended algorithms in the IANA registries [DNSKEY-IANA] [DS-IANA].

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

IANA has updated the SHA-1 (1) entry in the "Digest Algorithms" registry [DS-IANA] [RFC9904] as follows and has added this document as a reference for the entry:

Value: 1
Description: SHA-1
Use for DNSSEC Delegation: **MUST NOT**
Use for DNSSEC Validation: **RECOMMENDED**
Implement for DNSSEC Delegation: **MUST NOT**

Implement for DNSSEC Validation: **MUST**

IANA has updated the RSASHA1 (5) and RSASHA1-NSEC3-SHA1 (7) algorithm entries in the "DNS Security Algorithm Numbers" registry [DNSKEY-IANA] [RFC9904] as follows and has added this document as a reference for the entries:

Number: 5
Description: RSA/SHA-1
Mnemonic: RSASHA1
Zone Signing: Y
Trans. Sec.: Y
Use for DNSSEC Signing: **MUST NOT**
Use for DNSSEC Validation: **RECOMMENDED**
Implement for DNSSEC Signing: **NOT RECOMMENDED**
Implement for DNSSEC Validation: **MUST**

Number: 7
Description: RSASHA1-NSEC3-SHA1
Mnemonic: RSASHA1-NSEC3-SHA1
Zone Signing: Y
Trans. Sec.: Y
Use for DNSSEC Signing: **MUST NOT**
Use for DNSSEC Validation: **RECOMMENDED**
Implement for DNSSEC Signing: **NOT RECOMMENDED**
Implement for DNSSEC Validation: **MUST**

6. Normative References

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

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

[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>.

[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/info/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/info/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/info/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/info/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/info/rfc8174>.

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

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

[RFC9904] Hardaker, W. and W. Kumari, "DNSSEC Cryptographic Algorithm Recommendation Update Process", RFC 9904, DOI 10.17487/RFC9904, November 2025, <https://www.rfc-editor.org/info/rfc9904>.

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 specification.

Authors' Addresses

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

Warren Kumari
Google
Email: warren@kumari.net