Stream: Internet Engineering Task Force (IETF)
RFC: 9904
Obsoletes: 8624
Updates: 9157
Category: Standards Track
Published: October 2025
ISSN: 2070-1721
Authors: W. Hardaker, *USC/ISI*
W. Kumari, *Google*

RFC 9904
DNSSEC Cryptographic Algorithm Recommendation Update Process

Abstract

The DNSSEC protocol makes use of various cryptographic algorithms to provide authentication of DNS data and proof of nonexistence. To ensure interoperability between DNS resolvers and DNS authoritative servers, it is necessary to specify both a set of algorithm implementation requirements and usage guidelines to ensure that there is at least one algorithm that all implementations support. This document replaces and obsoletes RFC 8624 and moves the canonical source of algorithm implementation requirements and usage guidance for DNSSEC from RFC 8624 to the IANA DNSSEC algorithm registries. This is done to allow the list of requirements to be more easily updated and referenced. Extensions to these registries can be made in future RFCs. This document also updates RFC 9157 and incorporates the revised IANA DNSSEC considerations from that RFC.

This document does not change the recommendation status (**MUST**, **MAY**, **RECOMMENDED**, etc.) of the algorithms listed in RFC 8624; that is the work of future documents.

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/rfc9904.

Copyright Notice

Table of Contents

1. Introduction 3
1.1. Document Audience 4
1.2. Updating Algorithm Requirement Levels 4
1.3. Requirements Notation 5
2. Adding Usage and Implementation Recommendations to the IANA DNSSEC Algorithm Registries 5
2.1. Column Descriptions 6
2.2. Adding and Changing Values 6
3. DNS Security Algorithm Numbers Registry Column Values 8
4. Digest Algorithms Registry Column Values 9
5. Security Considerations 9
6. Operational Considerations 10
7. IANA Considerations 10
7.1. Update to the DNS Security Algorithm Numbers Registry 10
7.2. Update to the Digest Algorithms Registry 11
8. References 11
8.1. Normative References 11
8.2. Informative References 12
Acknowledgments 13
Authors' Addresses 13

1. Introduction

"DNS Security Extensions (DNSSEC)" [RFC9364] is used to provide authentication of DNS data. The DNSSEC signing algorithms are defined by various RFCs, including [RFC4034], [RFC4509], [RFC5155], [RFC5702], [RFC5933], [RFC6605], and [RFC8080].

To ensure interoperability, a set of "mandatory-to-implement" DNS Public Key (DNSKEY) algorithms are defined in [RFC8624]. To make the current status of the algorithms more easily accessible and understandable, and to make future changes to these recommendations easier to

publish, this document moves the canonical status of the algorithms from [RFC8624] to the IANA DNSSEC algorithm registries. Additionally, as advice to operators, it adds recommendations for deploying and using these algorithms.

This is similar to the process used for the "TLS Cipher Suites" registry [TLS-ciphersuites], where the canonical list of cipher suites is in the IANA registry, and RFCs reference the IANA registry.

1.1. Document Audience

The columns added to the IANA "DNS Security Algorithm Numbers" [DNSKEY-IANA] and "Digest Algorithms" [DS-IANA] registries target DNSSEC operators and implementers.

Implementations need to meet high security expectations as well as provide interoperability between various implementations and with different versions.

The field of cryptography evolves continuously. New, stronger algorithms appear, and existing algorithms may be found to be less secure than originally thought. Therefore, algorithm implementation requirements and usage guidance need to be updated from time to time in order to reflect the new reality and to allow for a smooth transition to more secure algorithms as well as the deprecation of algorithms deemed to no longer be secure.

Implementations need to be conservative in the selection of algorithms they implement in order to minimize both code complexity and the attack surface.

The perspective of implementers may differ from that of an operator who wishes to deploy and configure DNSSEC with only the safest algorithm. As such, this document also adds new recommendations about which algorithms should be deployed regardless of implementation status. In general, it is expected that deployment of aging algorithms should generally be reduced before implementations stop supporting them.

1.2. Updating Algorithm Requirement Levels

By the time a DNSSEC cryptographic algorithm is made mandatory to implement, it should already be available in most implementations. This document defines an IANA registration modification to allow future documents to specify the implementation recommendations for each algorithm, as the recommendation status of each DNSSEC cryptographic algorithm is expected to change over time. For example, there is no guarantee that newly introduced algorithms will become mandatory to implement in the future. Likewise, published algorithms are continuously subjected to cryptographic attack and may become too weak, or even be completely broken, and will require deprecation in the future.

It is expected that the deprecation of an algorithm will be performed gradually. This provides time for implementations to update their implemented algorithms while remaining interoperable. Unless there are strong security reasons, an algorithm is expected to be downgraded from **MUST** to **NOT RECOMMENDED** or **MAY**, instead of directly from **MUST** to **MUST NOT**. Similarly, an algorithm that has not been mentioned as mandatory to implement is expected to be first introduced as **RECOMMENDED** instead of a **MUST**.

Since the effect of using an unknown DNSKEY algorithm is that the zone is treated as insecure, it is recommended that algorithms that have been downgraded to **NOT RECOMMENDED** or lower not be used by authoritative nameservers and DNSSEC signers to create new DNSKEYs. This ensures that the use of deprecated algorithms decreases over time. Once an algorithm has reached a sufficiently low level of deployment, it can be marked as **MUST NOT**, so that recursive resolvers can remove support for validating it.

Validating recursive resolvers are encouraged to retain support for all algorithms not marked as **MUST NOT**.

1.3. 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.

[RFC2119] considers the term **SHOULD** to be equivalent to **RECOMMENDED**, and **SHOULD NOT** equivalent to **NOT RECOMMENDED**. This document has chosen to use the terms **RECOMMENDED** and **NOT RECOMMENDED**, as this more clearly expresses the recommendations to implementers.

2. Adding Usage and Implementation Recommendations to the IANA DNSSEC Algorithm Registries

Per this document, the following columns have been added to the corresponding DNSSEC algorithm registries maintained by IANA:

Registry	Column Added
DNS Security Algorithm Numbers	Use for DNSSEC Signing
DNS Security Algorithm Numbers	Use for DNSSEC Validation
DNS Security Algorithm Numbers	Implement for DNSSEC Signing
DNS Security Algorithm Numbers	Implement for DNSSEC Validation
Digest Algorithms	Use for DNSSEC Delegation
Digest Algorithms	Use for DNSSEC Validation
Digest Algorithms	Implement for DNSSEC Delegation
Digest Algorithms	Implement for DNSSEC Validation

Table 1: Columns Added to Existing DNSSEC Algorithm Registries

2.1. Column Descriptions

The intended usage of the four columns in the "DNS Security Algorithm Numbers" registry is as follows:

Use for DNSSEC Signing: Indicates the recommendation for using the algorithm within authoritative servers.

Use for DNSSEC Validation: Indicates the recommendation for using the algorithm in DNSSEC validators.

Implement for DNSSEC Signing: Indicates the recommendation for implementing the algorithm within DNSSEC signing software.

Implement for DNSSEC Validation: Indicates the recommendation for implementing the algorithm within DNSSEC validators.

The intended usage of the four columns in the "Digest Algorithms" registry is as follows:

Use for DNSSEC Delegation: Indicates the recommendation for using the algorithm within authoritative servers.

Use for DNSSEC Validation: Indicates the recommendation for using the algorithm in DNSSEC validators.

Implement for DNSSEC Delegation: Indicates the recommendation for implementing the algorithm within authoritative servers.

Implement for DNSSEC Validation: Indicates the recommendation for implementing the algorithm within validating resolvers.

2.2. Adding and Changing Values

The following note describing the procedures for adding and changing values has been added to the "DNS Security Algorithm Numbers" registry:

> Adding a new entry to the "DNS Security Algorithm Numbers" registry with a recommended value of "**MAY**" in the "Use for DNSSEC Signing", "Use for DNSSEC Validation", "Implement for DNSSEC Signing", or "Implement for DNSSEC Validation" columns will be subject to the Specification Required policy as defined in [RFC8126] in order to promote continued evolution of DNSSEC algorithms and DNSSEC agility. New entries added through the Specification Required process will have the value of "**MAY**" for all columns.

> Adding a new entry to, or changing an existing value in, the "DNS Security Algorithm Numbers" registry that has any value other than "**MAY**" in the "Use for DNSSEC Signing", "Use for DNSSEC Validation", "Implement for DNSSEC Signing", or "Implement for DNSSEC Validation" columns requires Standards Action.
>
> If an item is not marked as "**RECOMMENDED**", it does not necessarily mean that it is flawed; rather, it indicates that the item either has not been through the IETF consensus process, has limited applicability, or is intended only for specific use cases.

The following note has been added to the "Digest Algorithms" registry:

> Adding a new entry to the "Digest Algorithms" registry with a recommended value of "**MAY**" in the "Use for DNSSEC Delegation", "Use for DNSSEC Validation", "Implement for DNSSEC Delegation", or "Implement for DNSSEC Validation" columns **SHALL** follow the Specification Required policy as defined in [RFC8126].
>
> Adding a new entry to, or changing an existing value in, the "Digest Algorithms" registry that has any value other than "**MAY**" in the "Use for DNSSEC Delegation", "Use for DNSSEC Validation", "Implement for DNSSEC Delegation", or "Implement for DNSSEC Validation" columns requires Standards Action.
>
> If an item is not marked as "**RECOMMENDED**", it does not necessarily mean that it is flawed; rather, it indicates that the item either has not been through the IETF consensus process, has limited applicability, or is intended only for specific use cases.

Only values of "**MAY**", "**RECOMMENDED**", "**MUST NOT**", and "**NOT RECOMMENDED**" may be placed into the "Use for DNSSEC Signing" and "Use for DNSSEC Validation" columns. Only values of "**MAY**", "**RECOMMENDED**", "**MUST**", "**MUST NOT**", and "**NOT RECOMMENDED**" may be placed into the "Implement for DNSSEC Signing" and "Implement for DNSSEC Validation" columns. Note that a value of "**MUST**" is not an allowed value for the two "Use for" columns.

The following sections state the initial values that have been populated into these columns. The values in the "Implement for" columns are transcribed from [RFC8624]. The "Use for" columns are set to the same values as those in the "Implement for" columns since the general interpretation to date indicates they have been treated as values for both "use" and "implementation". Note that the value in the "Use for" column is "**RECOMMENDED**" when the value in the corresponding "Implement for" column is "**MUST**". We note that the values for "Implement for" and "Use for" may diverge in the future as implementations generally precede deployments.

3. DNS Security Algorithm Numbers Registry Column Values

Initial values for the use and implementation recommendation columns in the "DNS Security Algorithm Numbers" registry under the "Domain Name System Security (DNSSEC) Algorithm Numbers" registry group are shown in Table 2.

When there are multiple **RECOMMENDED** algorithms in the "Use for" columns, operators should choose the best algorithm according to local policy.

No.	Mnemonics	Use for DNSSEC Signing	Use for DNSSEC Validation	Implement for DNSSEC Signing	Implement for DNSSEC Validation
1	RSAMD5	**MUST NOT**	**MUST NOT**	**MUST NOT**	**MUST NOT**
3	DSA	**MUST NOT**	**MUST NOT**	**MUST NOT**	**MUST NOT**
5	RSASHA1	**NOT RECOMMENDED**	**RECOMMENDED**	**NOT RECOMMENDED**	**MUST**
6	DSA-NSEC3-SHA1	**MUST NOT**	**MUST NOT**	**MUST NOT**	**MUST NOT**
7	RSASHA1-NSEC3-SHA1	**NOT RECOMMENDED**	**RECOMMENDED**	**NOT RECOMMENDED**	**MUST**
8	RSASHA256	**RECOMMENDED**	**RECOMMENDED**	**MUST**	**MUST**
10	RSASHA512	**NOT RECOMMENDED**	**RECOMMENDED**	**NOT RECOMMENDED**	**MUST**
12	ECC-GOST	**MUST NOT**	**MAY**	**MUST NOT**	**MAY**
13	ECDSAP256SHA256	**RECOMMENDED**	**RECOMMENDED**	**MUST**	**MUST**
14	ECDSAP384SHA384	**MAY**	**RECOMMENDED**	**MAY**	**RECOMMENDED**
15	ED25519	**RECOMMENDED**	**RECOMMENDED**	**RECOMMENDED**	**RECOMMENDED**
16	ED448	**MAY**	**RECOMMENDED**	**MAY**	**RECOMMENDED**
17	SM2SM3	**MAY**	**MAY**	**MAY**	**MAY**
23	ECC-GOST12	**MAY**	**MAY**	**MAY**	**MAY**
253	PRIVATEDNS	**MAY**	**MAY**	**MAY**	**MAY**

No.	Mnemonics	Use for DNSSEC Signing	Use for DNSSEC Validation	Implement for DNSSEC Signing	Implement for DNSSEC Validation
254	PRIVATEOID	**MAY**	**MAY**	**MAY**	**MAY**

Table 2: Initial Values for the DNS Security Algorithm Numbers Registry Columns

4. Digest Algorithms Registry Column Values

Initial values for the use and implementation recommendation columns in the "Digest Algorithms" registry under the "DNSSEC Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms" registry group are shown in Table 3.

When there are multiple **RECOMMENDED** algorithms in the "Use for" columns, operators should choose the best algorithm according to local policy.

Value	Description	Use for DNSSEC Delegation	Use for DNSSEC Validation	Implement for DNSSEC Delegation	Implement for DNSSEC Validation
0	NULL (CDS only)	**MUST NOT**	**MUST NOT**	**MUST NOT**	**MUST NOT**
1	SHA-1	**MUST NOT**	**RECOMMENDED**	**MUST NOT**	**MUST**
2	SHA-256	**RECOMMENDED**	**RECOMMENDED**	**MUST**	**MUST**
3	GOST R 34.11-94	**MUST NOT**	**MAY**	**MUST NOT**	**MAY**
4	SHA-384	**MAY**	**RECOMMENDED**	**MAY**	**RECOMMENDED**
5	GOST R 34.11-2012	**MAY**	**MAY**	**MAY**	**MAY**
6	SM3	**MAY**	**MAY**	**MAY**	**MAY**

Table 3: Initial Values for the Digest Algorithms Registry Columns

5. Security Considerations

The security of cryptographic systems depends on the strength of both the cryptographic algorithms chosen and the keys used with those algorithms. The security also depends on the engineering of the protocol used by the system to ensure that there are no non- cryptographic ways to bypass the security of the overall system.

This document concerns itself with the selection of cryptographic algorithms for the use of DNSSEC, specifically with the selection of "mandatory-to-implement" algorithms. In this document, the algorithms identified as **MUST** or **RECOMMENDED** to implement are not known to be broken at the current time, and cryptographic research so far leads us to believe that they are likely to remain adequately secure unless significant and unexpected discovery is made. However, this isn't necessarily forever, and it is expected that future documents will be issued from time to time to reflect the current best practices in this area.

Retiring an algorithm too soon would result in a zone signed with the retired algorithm being downgraded to the equivalent of an unsigned zone. Therefore, algorithm deprecation must be done only after careful consideration and ideally slowly when possible.

6. Operational Considerations

DNSKEY algorithm rollover in a live zone is a complex process. See [RFC6781] and [RFC7583] for guidelines on how to perform algorithm rollovers.

DS algorithm rollover in a live zone is also a complex process. Upgrading an algorithm at the same time as rolling to the new Key Signing Key (KSK) key will lead to DNSSEC validation failures, and users **MUST** upgrade the DS algorithm first before rolling to a new KSK.

7. IANA Considerations

IANA has updated the "DNS Security Algorithm Numbers" [DNSKEY-IANA] and "Digest Algorithms" [DS-IANA] registries according to the sections that follow.

7.1. Update to the DNS Security Algorithm Numbers Registry

IANA has updated the "DNS Security Algorithm Numbers" registry [DNSKEY-IANA] with the following columns and has populated these columns with the values from Table 2 of this document:

- "Use for DNSSEC Signing"
- "Use for DNSSEC Validation"
- "Implement for DNSSEC Signing"
- "Implement for DNSSEC Validation"

Additionally, IANA has completed the following actions for the "DNS Security Algorithm Numbers" registry [DNSKEY-IANA]:

- Changed the registration procedure to Standards Action or Specification Required.
- Added a note to the registry that describes the values not marked as "**RECOMMENDED**" per Section 2.2.
- Listed this document as an additional reference for the registry.

7.2. Update to the Digest Algorithms Registry

IANA has updated the "Digest Algorithms" registry [DS-IANA] with the following columns and has populated these columns with the values from Table 3 of this document:

- "Use for DNSSEC Delegation"
- "Use for DNSSEC Validation"
- "Implement for DNSSEC Delegation"
- "Implement for DNSSEC Validation"

Additionally, IANA has completed the following actions for the "Digest Algorithms" registry [DS-IANA]:

- Changed the registration procedure to Standards Action or Specification Required.
- Added a note to the registry that describes the values not marked as "**RECOMMENDED**" per Section 2.2.
- Listed this document as an additional reference for the registry.
- Marked values 128-252 as "Reserved".
- Marked values 253 and 254 as "Reserved for Private Use".
- Deleted the (now superfluous) column "Status" from the registry.

8. References

8.1. Normative References

[DNSKEY-IANA] IANA, "DNS Security Algorithm Numbers", <https://www.iana.org/assignments/dns-sec-alg-numbers>.

[DS-IANA] IANA, "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>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[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>.

[RFC9157] Hoffman, P., "Revised IANA Considerations for DNSSEC", RFC 9157, DOI 10.17487/RFC9157, December 2021, <https://www.rfc-editor.org/info/rfc9157>.

8.2. Informative References

[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>.

[RFC4509] Hardaker, W., "Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)", RFC 4509, DOI 10.17487/RFC4509, May 2006, <https://www.rfc-editor.org/info/rfc4509>.

[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>.

[RFC5702] Jansen, J., "Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC", RFC 5702, DOI 10.17487/RFC5702, October 2009, <https://www.rfc-editor.org/info/rfc5702>.

[RFC5933] Dolmatov, V., Ed., Chuprina, A., and I. Ustinov, "Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC", RFC 5933, DOI 10.17487/RFC5933, July 2010, <https://www.rfc-editor.org/info/rfc5933>.

[RFC6605] Hoffman, P. and W.C.A. Wijngaards, "Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC", RFC 6605, DOI 10.17487/RFC6605, April 2012, <https://www.rfc-editor.org/info/rfc6605>.

[RFC6781] Kolkman, O., Mekking, W., and R. Gieben, "DNSSEC Operational Practices, Version 2", RFC 6781, DOI 10.17487/RFC6781, December 2012, <https://www.rfc-editor.org/info/rfc6781>.

[RFC7583] Morris, S., Ihren, J., Dickinson, J., and W. Mekking, "DNSSEC Key Rollover Timing Considerations", RFC 7583, DOI 10.17487/RFC7583, October 2015, <https://www.rfc-editor.org/info/rfc7583>.

[RFC8080] Sury, O. and R. Edmonds, "Edwards-Curve Digital Security Algorithm (EdDSA) for DNSSEC", RFC 8080, DOI 10.17487/RFC8080, February 2017, <https://www.rfc-editor.org/info/rfc8080>.

[RFC8624] Wouters, P. and O. Sury, "Algorithm Implementation Requirements and Usage Guidance for DNSSEC", RFC 8624, DOI 10.17487/RFC8624, June 2019, <https://www.rfc-editor.org/info/rfc8624>.

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

[TLS-ciphersuites] IANA, "Transport Layer Security (TLS) Parameters", <https://www.iana.org/assignments/tls-parameters>.

Acknowledgments

This document is based on, and extends, RFC 8624, which was authored by Paul Wouters and Ondrej Sury.

The content of this document was heavily discussed by participants of the DNSOP Working Group. The authors appreciate the thoughtfulness of the many opinions expressed by working group participants that all helped shaped this document. We thank Paul Hoffman and Paul Wouters for their contributed text and also Nabeel Cocker, Shumon Huque, Nicolai Leymann, S. Moonesamy, Magnus Nyström, Peter Thomassen, Stefan Ubbink, and Loganaden Velvindron for their reviews and comments.

Authors' Addresses

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

Warren Kumari
Google
Email: warren@kumari.net