Network Working Group
Internet-Draft
Obsoletes: 8624 (if approved)
Updates: 9157 (if approved)
Intended status: Standards Track
Expires: 6 December 2025

W. Hardaker
USC/ISI
W. Kumari
Google

4 June 2025

DNSSEC Cryptographic Algorithm Recommendation Update Process
draft-ietf-dnsop-rfc8624-bis-13

Abstract

The DNSSEC protocol makes use of various cryptographic algorithms to provide authentication of DNS data and proof of non-existence. 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 RFC8624 and moves the canonical source of algorithm implementation requirements and usage guidance for DNSSEC from RFC8624 to an IANA registry. This is done both to allow the list of requirements to be more easily updated, and to allow the list to be more easily referenced. Future extensions to this registry can be made under new, incremental update RFCs. This document also incorporates the revised IANA DNSSEC considerations from RFC9157.

The document does not change the status (MUST, MAY, RECOMMENDED, etc.) of the algorithms listed in RFC8624; that is the work of future documents.

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 6 December 2025.

Table of Contents

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], [RFC8080].

To ensure interoperability, a set of "mandatory to implement" 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 the usage of these algorithms.

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

1.1. Document Audience

The columns added to the IANA "DNS Security Algorithm Numbers" [DNSKEY-IANA] and "DNSSEC Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms" [DS-IANA] registries target DNSSEC operators and implementers.

Implementations need to meet both 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 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 which have been downgraded to NOT RECOMMENDED or lower not be used by authoritative nameservers and DNSSEC signers to create new DNSKEY’s. 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 registries

Per this document, the following columns are being added to the following DNSSEC algorithm registries maintained with 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 Algorithm	Use for DNSSEC Delegation
Digest Algorithm	Use for DNSSEC Validation
Digest Algorithm	Implement for DNSSEC Delegation
Digest Algorithm	Implement for DNSSEC Validation

Table 1: Columns to add to existing DNSSEC algorithm registries

2.1. Column Descriptions

The intended usage of the four columns in the "DNS Security Algorithm Numbers" table are:

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 Algorithm" table are:

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

Adding a new entry to the "DNS System 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 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. (Ed note (RFC Editor - please delete this before publication): As a reminder: the "Specification Required" policy includes a requirement for a designated expert to review the request.)

Adding a new entry to, or changing existing values in, the "DNS System Algorithm Numbers" registry for the "Use for DNSSEC Signing", "Use for DNSSEC Validation", "Implement for DNSSEC Signing", or "Implement for DNSSEC Validation" columns to any other value than "MAY" requires a Standards Action.

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 existing values in, the "DNS System Algorithm Numbers" registry for the "Use for DNSSEC Delegation", "Use for DNSSEC Validation", "Implement for DNSSEC Delegation", or "Implement for DNSSEC Validation" columns to any other value than "MAY" requires a 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 to be populated into these rows. The "Implement for" column values are transcribed from [RFC8624]. The "Use for" columns are set to the same values as the "Implement for" values since the general interpretation to date indicates they have been treated as values for both "implementation" and "use". Note that the "Use for" columns values use "RECOMMENDED" when the corresponding "Implement for" column is a "MUST" value. We note that the values for "Implement for" and "Use for" may diverge in the future as implementations generally precede deployments.

3. DNS System Algorithm Numbers Column Values

Initial recommendation columns of use and implementation recommendations for the "Domain Name System Security (DNSSEC) Algorithm Numbers" are shown in Table 2.

When there are multiple RECOMMENDED algorithms in the "use" column, operators should choose the best algorithm according to local policy.

N	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	SM2/SM3	MAY	MAY	MAY	MAY
23	GOST R 34.10-2012	MAY	MAY	MAY	MAY
253	private algorithm	MAY	MAY	MAY	MAY
254	private algorithm OID	MAY	MAY	MAY	MAY

Table 2: Initial values for the DNS System Algorithm Numbers columns

4. DNSSEC Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms Column Values

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

When there are multiple RECOMMENDED algorithms in the "use" column, operators should choose the best algorithm according to local policy.

Number	Mnemonics	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 DNSSEC Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms columns

5. Security Considerations

The security of cryptographic systems depends on both the strength of the cryptographic algorithms chosen and the strength of 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. The algorithms identified in this document 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 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

The IANA is requested to update the [DNSKEY-IANA] and [DS-IANA] registries according to the following sections.

7.1. Update to the "DNS Security Algorithm Numbers" registry

This document requests IANA update the "DNS Security Algorithm Numbers" registry ([DNSKEY-IANA]) registry with the following additional columns:

* "Use for DNSSEC Signing"

* "Use for DNSSEC Validation"

* "Implement for DNSSEC Signing"

* "Implement for DNSSEC Validation"

These values must be populated using values from Table 2 of this document.

Additionally, the registration policy for the [DNSKEY-IANA] registry should match the text describing the requirements in this document, and Section 2's note concerning values not marked as "RECOMMENDED" should be added to the registry.

This document should be listed as a reference to the "DNS Security Algorithm Numbers" registry.

7.2. Update to the "Digest Algorithms" registry

This document requests IANA update the "Digest Algorithms" registry ([DS-IANA]) registry with the following additional columns:

* "Use for DNSSEC Delegation"

* "Use for DNSSEC Validation"

* "Implement for DNSSEC Delegation"

* "Implement for DNSSEC Validation"

These values must be populated using values from Table 3 of this document.

* Update the registration policy for the [DS-IANA] registry to match the text describing update requirements above

* Mark values 128 - 252 as "Reserved"

* Mark values 253 and 254 as "Reserved for Private Use"

* Delete the (now superfluous) column "Status" from the registry

Section 2's note concerning values not marked as "RECOMMENDED" should be added to the registry.

This document should be listed as a reference to the "Digest Algorithms" registry.

8. 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 Nystr旦m, Peter Thomassen, Stefan Ubbink, and Loganaden Velvindron for their reviews and comments.

9. References

9.1. Normative References

[DNSKEY-IANA]
IANA, "DNS Security Algorithm Numbers", n.d., <https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml#dns-sec-alg-numbers-1>.

[DS-IANA] IANA, "Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms", n.d., <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/rfc/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/rfc/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/rfc/rfc8174>.

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

9.2. 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/rfc/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/rfc/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/rfc/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/rfc/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/rfc/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/rfc/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/rfc/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/rfc/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/rfc/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/rfc/rfc8624>.

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

[TLS-ciphersuites] IANA, "Transport Layer Security (TLS) Parameters", n.d., <https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4>.

Appendix A. ChangeLog

(RFC Editor: please remove this ChangeLog section upon publication.)

A.1. Changes from ietf-10 to ietf-11:

* Many more comments to address IESG reviews

A.2. Changes from ietf-09 to ietf-10:

* Many comments addressed from IESG reviews

A.3. Changes from ietf-08 to ietf-09

* Added missing alogirthms (SM2/SM3 and GOST R 34.10-2012)

A.4. Changes from ietf-07 to ietf-08

* Handle issues raised during IETF last call:
  * updates 9157
  * other nit fixes

A.5. Changes from ietf-06 to ietf-07

* changed to a standards track document

A.6. Changes from ietf-05 to ietf-06

* Address Eric Vyncke (RAD!) AD review comments.

A.7. Changes from ietf-03 to ietf-05

* Updated "entry requirements" to be "Specification Required".
* Marked values 128 - 252 as "Reserved" in "Digest Algorithms" as break-glass mechanism in case we get a flood of these. To align with the "DNS Security Algorithm Numbers" registry (that reserves 123 - ...)
* Marked values 253 and 254 as "Reserved for Private Use" in "Digest Algorithms"
* Deleted the (now superfluous) column "Status" from the "Digest

A.8. Changes from ietf-02 to ietf-03

* Fixed the reference in the Abstract (no links in Abstracts)

* Added Updates: to the header.

A.9. Changes from ietf-01 to ietf-02

* Changed the MUST values in the tables for the Use columns to RECOMMENDED based on discussions on the dnsop mailing list.

* Other minor wording and formatting changes

A.10. Changes from ietf-00 to ietf-01

* Only NIT fixing

A.11. Changes from hardaker-04 to ietf-00

* Just a draft name and number change.

A.12. Changes from -03 to -04

* Changed the columns being added from 2 per table to 4, based on discussion within the dnsop working group mailing list. This was a fairly major set of changes.

A.13. Changes since RFC8624

* The primary purpose of this revision is to introduce the new columns to existing registries. It makes no changes to the previously defined values.

* Merged in RFC9157 updates.

* Set authors as Wes Hardaker, Warren Kumari.

Authors' Addresses

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

Warren Kumari
Google
Email: warren@kumari.net