Domain Name System Operations
Internet-Draft
Intended status: Informational
Expires: 5 May 2026

S. Crocker
Edgemoor Research Institute
R. Housley
Vigil Security
W. Hardaker
Google

1 November 2025

Documenting and Managing DNSSEC Algorithm Lifecycles
draft-crocker-dnsop-dnssec-algorithm-lifecycle-02

Abstract

Cryptographic algorithms for DNSSEC go through multiple phases during their lifetime. They are created, tested, adopted, used, and deprecated over a period of time. This RFC defines phases for the DNSSEC algorithm lifecycle, and it defines the criteria for moving from one phase to the next.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-crocker-dnsop-dnssec-algorithm-lifecycle/.

Discussion of this document takes place on the Domain Name System Operations Working Group mailing list (mailto:dnsop@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/dnsop/. Subscribe at https://www.ietf.org/mailman/listinfo/dnsop/.

Source for this draft and an issue tracker can be found at https://github.com/russhousley/draft-crocker-dnsop-dnssec-algorithm-lifecycle.

Status of This Memo

Table of Contents

1. Background

Each DNSSEC cryptographic algorithm is used in two distinct but interconnected ways. The first is to sign. The second is to validate a signature. If someone uses an algorithm to sign, the party that receives that signed message should be able to validate the signature. This means the receiving parties need to implement the validation algorithm before the sending parties can expect to use it effectively. Equally, the receiving parties have to keep the validation algorithm in service even after the signing parties stop using it.

These relationships seem obvious, but there has not been an organized way to communicate within the Internet community regarding these algorithm transitions. This document builds upon the enhancements defined in [I-D.ietf-dnsop-rfc8624-bis] to the IANA "DNS Security Algorithm Numbers" registry [DNSKEY-IANA] and the IANA "DNSSEC Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms" registry [DS-IANA]; the values in these registries tell the phase that the algorithm is in with respect to this lifecycle. This document discusses both the expected phasing in and out of algorithms individually using these IANA registries, as well the need for how the DNSSEC ecosystem as a whole should ensure it is left in a resilient cryptographic state.

2. Seven phases in the lifecycle of a DNSSEC algorithm

We define seven phases in the lifecycle of an individual DNSSEC algorithm.

1. Experimental: The algorithm is under development by the cryptographic community and is not yet ready for general use.

2. Adopted: The algorithm is ready to be used by the Internet community. It is listed in the IANA registry. Implementers are expected to support the algorithm for signature validation.

3. Available: The algorithm is ready for use by all parties. Implementers are expected to support the algorithm for signing and signature validation.

4. Mainstream: The algorithm has reached "recommended" status. Implementers are expected to support the algorithm for signing and signature validation.

5. Phaseout: The algorithm is nearing the end of its lifecycle, but it is still in use. Implementers are advised to transition to other recommended algorithms. Signing should be phased out.

6. Deprecated: All use for signing should have stopped, but signature validation is still supported.

7. Obsolete: No support for signing or signature validation is expected.

3. Process and Criteria for transitions

The previous section does not specify the process and criteria for advancing a DNSSEC algorithm through these lifecycle phases. There are six transition points, labelled A through F, between these seven lifecycle phases. We propose the following process and criteria for these transitions.

A. Algorithm Inclusion

* Prerequisites:

  - Algorithm has been given a Mnemonic and number in the "DNS Security Algorithm Numbers" registry.

  - Cryptographic community has determined that the algorithm as suitable to use for DNSSEC.

  - Documentation and implementations are widely available and stable.

* IETF determines the algorithm is suitable for use with DNSSEC.

* Action: IETF publishes notice that the algorithm is suitable for use and should be deployed for signature validation.

B. Ready for Use

* Prerequisites:

  - Deployment has been measured.

  - Deployment is deemed to have reached an acceptable level.

* IETF reaches consensus that algorithm has been widely deployed for DNSSEC.

* Action: IETF publishes notice that algorithm is available for DNSSEC signing.

C. Mainstream

* IETF reaches consensus that algorithm has reached mainstream status; deployment is essentially universal.

* Actions:

- IETF publishes notice that algorithm has reached mainstream status.

- Signers using older algorithms, particularly algorithms in the Phaseout or later phases should transition to a mainstream algorithm.

D. Phaseout

* Prerequisites:

  - Cryptographic community has determined the algorithm is reaching its end of life.

* IETF determines it is time to announce the phaseout.

* Action: IETF publishes notice to signing operators to transition away from the algorithm and begin signing with a mainstream algorithm.

E. Deprecation

* Prerequisites:

  - Measure signing activity.

  - Signing activity is deemed to have largely subsided.

* IETF determines it is time to deprecate the algorithm for use with DNSSEC.

* Action: IETF publishes notice that use of the algorithm is now inappropriate for DNSSEC signing.

F. Obsolescence

* Prerequisite: Measurement of signing is at the lowest achievable level.

* IETF determines the algorithm is obsolete.

* Action: IETF publishes notice that algorithm is obsolete and ought be removed from implementations.

4. Lifecycle Phase and the IANA Registry

The enhancements to the IANA registry of DNSSEC algorithms defined in [I-D.ietf-dnsop-rfc8624-bis]. Table 1 suggests the values to be placed into each of the IANA registry columns "Use for DNSSSEC Signing", "Use for DNSSSEC Validation", "Implement for DNSSSEC Signing", and "Implement for DNSSSEC Validation" for each phase in the algorithms lifecycle defined in Section 2. The IETF is encouraged to follow Table 1 when assigning the values in both of these IANA registries algorithms as each algorithm progresses through the lifecycle.

	DNSSEC Validation		DNSSEC Signing	
Phase	Implement	Use	Implement	Use
1	MAY	MAY	MAY	MAY
2	RECOMMENDED	MAY	RECOMMENDED	MAY
3	MUST	RECOMMENDED	MUST	MAY
4	MUST	MUST	MUST	RECOMMENDED
5	MUST	RECOMMENDED	RECOMMENDED	NOT RECOMMENDED
6	RECOMMENDED	NOT RECOMMENDED	NOT RECOMMENDED	MUST NOT
7	NOT RECOMMENDED -- or -- MUST NOT	MUST NOT	MUST NOT	MUST NOT

Table 1. Determine lifecycle phase from the IANA registry.

5. Considerations for maintaining a robust DNSSEC algorithm state

The above considers the values associated with a particular algorithm in the IANA registry for "DNS Security Algorithm Numbers" [DNSKEY-IANA] and the IANA registry for "DNSSEC Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms" [DS-IANA]. It is equally as important to ensure that as algorithms come into favor and out of favor that the current set of available algorithms always include some that are the Mainstream state. As the IETF community considers transitioning a particular algorithm beyond the Mainstream state, it must simultaneously ensure that at least one other algorithm is already present in the Mainstream state or that one other algorithm is in the Ready to Use state and available to become a Mainstream algorithm. Specifically, at no time should there be zero algorithms in the Mainstream state.

6. IANA Considerations

IANA is asked to amend the [DNSKEY-IANA] and [DS-IANA] registries to show the current phase of each algorithm. In addition, IANA is asked to show the history of future transitions through each phase.

The IESG is asked to name a panel of at least three designated experts (see Section 5 of [RFC8126]) to advise IANA when an algorithm is under consideration to be moved from one phase to the next. These designated experts should be familiar with hash functions, digital signature algorithms, and the DSNSEC protocol.

IANA has no actions related to this document.

7. Security Considerations

This document proposes a lifecycle for DNSSEC algorithms. By following the criteria presented in Section 3, Internet-wide deployment of new DNSSEC algorithm will occur in a smooth manner that ensures all implementations will be able to validate signatures. Likewise, following the criteria will ensure that out-of-date DNSSEC algorithm are retired in a graceful manner. The criteria associated with the transition between phases of the lifecycle will depend on the process that makes changes to the IANA registry as defined in [I-D.ietf-dnsop-rfc8624-bis].

If the industry fails to achieve global consensus on the state of any one algorithm such that domain owners deploying signing zones disagree with the deployed validating resolvers then it likely that DNS resolutions will fail, rendering the DNS unusable. As such, vendors of both authoritative and recursive resolvers, and the operating systems that deploy them, are encouraged to strictly follow the current guidance to avoid DNS interoperability issues.

8. References

8.1. Normative References

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

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

[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>.

8.2. Informative References

[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>.

Acknowledgments

Thanks to Wes Hardaker and Warren Kumari for constructive comments.

Authors' Addresses

Steve Crocker
Edgemoor Research Institute
Email: steve@shinkuro.com

Russ Housley
Vigil Security, LLC
Email: housley@vigilsec.com

Wes Hardaker
Google, LLC
Email: ietf@hardakers.net