Workgroup: Network Working Group
Internet-Draft:
draft-ietf-dnsop-dnssec-iana-cons-05
Updates: 5155, 6014, 8624 (if approved)
Published: 7 October 2021
Intended Status: Standards Track
Expires: 10 April 2022
Authors: P. Hoffman
         ICANN

Revised IANA Considerations for DNSSEC

Abstract

This document changes the review requirements needed to get DNSSEC
algorithms and resource records added to IANA registries. It updates
RFC 6014 to include hash algorithms for DS (Delegation Signer)
records and NSEC3 (Hashed Authenticated Denial of Existence)
parameters. It also updates RFC 5155 and RFC 6014, which have
requirements for DNSSEC algorithms, and updates RFC 8624 to say that
algorithms that are described in RFCs that are not on standards
track are only at the "MAY" level of implementation recommendation.
The rationale for these changes is to bring the requirements for DS
records and for the hash algorithms used in NSEC3 in line with the
requirements for all other DNSSEC 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 10 April 2022.

Copyright Notice

Table of Contents

1. Introduction

DNSSEC is primarily described in [RFC4033], [RFC4034], and [RFC4035]. DNSSEC commonly uses another resource record beyond those defined in RFC 4034: NSEC3 [RFC5155]. DS resrouce records were originally defined in [RFC3658], and that definition was obsoleted by RFC 4034.

[RFC6014] updated the requirements for how DNSSEC cryptographic algorithm identifiers in the IANA registries are assigned, reducing the requirements from being "Standards Action" to "RFC Required". However, the IANA registry requirements for hash algorithms for DS records [RFC3658] and for the hash algorithms used in NSEC3 records [RFC5155] are still "Standards Action". This document updates those IANA registry requirements. (For reference on how IANA registries can be updated in general, see [RFC8126].)

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. Update to RFC 6014

Section 4 updates RFC 6014 to bring the requirements for DS records and NSEC3 hash algorithms in line with the rest of the DNSSEC cryptographic algorithms by allowing any DS hash algorithms, NSEC3 hash algorithms, NSEC3 parameters, and NSEC3 flags that are fully

described in an RFC to have identifiers assigned in the IANA
registries. This is an addition to the IANA considerations in RFC
6014.

3. Update to RFC 8624

This document updates [RFC8624] for all DNSKEY and DS algorithms
that are not on standards track.

The second paragraph of Section 1.2 of RFC 8624 currently says:

This document only provides recommendations with respect to
mandatory-to-implement algorithms or algorithms so weak that they
cannot be recommended. Any algorithm listed in the [DNSKEY-IANA]
and [DS-IANA] registries that are not mentioned in this document
MAY be implemented. For clarification and consistency, an
algorithm will be specified as MAY in this document only when it
has been downgraded from a MUST or a RECOMMENDED to a MAY.

That paragraph is now replaced with the following:

This document provides recommendations with respect to
mandatory-to-implement algorithms, algorithms so weak that they
cannot be recommended, and algorithms that are defined in RFCs
that are not on standards track. Any algorithm listed in the
[DNSKEY-IANA] and [DS-IANA] registries that are not mentioned in
this document MAY be implemented. For clarification and
consistency, an algorithm will be specified as MAY in this
document only when it has been downgraded from a MUST or a
RECOMMENDED to a MAY.

This update is also reflected in the IANA considerations in Section
4.

4. IANA Considerations

In the "Domain Name System Security (DNSSEC) NextSECure3 (NSEC3)
Parameters" registry, the registration procedure for "DNSSEC NSEC3
Flags", "DNSSEC NSEC3 Hash Algorithms", and "DNSSEC NSEC3PARAM
Flags" are changed from "Standards Action" to "RFC Required".

In the "Delegation Signer (DS) Resource Record (RR) Type Digest
Algorithms" registry, the registration procedure for "Digest
Algorithms" is changed from "Standards Action" to "RFC Required".

5. Security Considerations

Changing the requirements for getting security algorithms added to
IANA registries as described in this document will make it easier to
get good algorithms added to the registries, and will make it easier

to get bad algorithms added to the registries. It is impossible to weigh the security impact of those two changes.

Administrators of DNSSEC-signed zones, and of validating resolvers, may have been making security decisions based on the contents of the IANA registries. This was a bad idea in the past, and now is an even worse idea because there will be more algorithms in those registries that may not have gone through IETF review. Security decisions about which algorithms are safe and not safe should be made by reading the security literature, not by looking in IANA registries.

6. References

6.1. Normative References

[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>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[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>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <https://www.rfc-editor.org/info/rfc4035>.

[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>.

[RFC6014] Hoffman, P., "Cryptographic Algorithm Identifier Allocation for DNSSEC", RFC 6014, DOI 10.17487/RFC6014, November 2010, <https://www.rfc-editor.org/info/rfc6014>.

[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>.

[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>.

6.2. Informative References

[RFC3658] Gudmundsson, O., "Delegation Signer (DS) Resource Record
           (RR)", RFC 3658, DOI 10.17487/RFC3658, December 2003,
           <https://www.rfc-editor.org/info/rfc3658>.

Appendix A. Acknowledgements

Donald Eastlake, Murray Kucherawy, Dan Harkins, Martin Duke, and
Benjamin Kaduk contributed to this document.

Author's Address

Paul Hoffman
ICANN

Email: paul.hoffman@icann.org