

Network Working Group
Internet-Draft
Updates: RFC [3658](#), [RFC 5155](#), [RFC 6014](#)
(if approved)
Intended status: Standards Track
Expires: January 7, 2021

P. Hoffman
ICANN
July 06, 2020

**Revised IANA Considerations for DNSSEC
draft-hoffman-dnssec-iana-cons-01**

Abstract

This document changes the review requirements needed to get some DNSSEC algorithms and resource records added to IANA registries. It updates [RFC 6014](#) to include hash algorithms for DS records and NSEC3 parameters.

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 January 7, 2021.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in [Section 4.e](#) of

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

- [1.](#) Introduction [2](#)
- [2.](#) IANA Considerations [2](#)
- [3.](#) Security Considerations [2](#)
- [4.](#) Normative References [3](#)
- [Appendix A.](#) Other Options for Requirements Level [3](#)
- Author's Address [4](#)

1. Introduction

DNSSEC is primarily described in [[RFC4033](#)], [[RFC4034](#)], and [[RFC4035](#)]. DNSSEC commonly uses two resource records beyond those defined in [RFC 4034](#): DS [[RFC3658](#)] and NSEC3 [[RFC5155](#)].

[RFC8126] describes the requirements for listing in the myriad IANA registries.

[RFC6014] updated the requirements for how DNSSEC cryptographic algorithm identifiers in the IANA registries are allocated, reducing the requirements from being "Standards Action" to "RFC Required". However, the IANA registry requirements for hash algorithms for DS records and for the hash algorithms used in NSEC3 are still "Standards Action". This document updates [RFC 6014](#) to bring the requirements for DS records and NSEC3 hash algorithms in line with the rest of the DNSSEC cryptographic algorithms.

2. 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".

3. 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.

4. Normative 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>>.
- [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>>.

Appendix A. Other Options for Requirements Level

During an early discussion in the DNSOP Working Group, it was proposed that the requirements for registry allocation for DS resource records be "Specification Required". This would reduce the work required of specification authors, and of the RFC Editor, while still requiring review by an expert reviewer and a long-lived specification.

Author's Address

Paul Hoffman
ICANN

Email: paul.hoffman@icann.org