Network Working Group
Internet-Draft
Updates: 2535, 3755, 4034
(if approved)
Intended status: Standards Track
Expires: September 23, 2010

P. Hoffman
VPN Consortium

March 22, 2010

Cryptographic Algorithm Identifier Allocation for DNSSEC
draft-ietf-dnsext-dnssec-alg-allocation-03

Abstract

This document specifies how DNSSEC cryptographic algorithm identifiers in the IANA registries are allocated. It changes the requirement from "standard required" to "RFC required". It does not change the list of algorithms that are recommended or required for DNSSEC implementations.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on September 23, 2010.

1. Introduction

[RFC2535] specifies that that IANA registry for DNS Security Algorithm Numbers be updated by IETF Standards Action only, with the exception of two values 253 and 254. In essence, this means that for an algorithm to get its own entry in the registry, the algorithm must be defined in an RFC on the Standards Track as defined in [RFC2026]. The requirement from RFC 2535 is repeated in [RFC3755] and [RFC4034].

RFC 2535 allows algorithms that are not on the Standards Track to use private values 253 and 254 in signatures. In each case, an unregistered private name must be included with each use of the algorithm in order to differentiate different algorithms that use the value.

2. Requirements for Assignments in the DNS Security Algorithm Numbers Registry

This document changes the requirement for registration from requiring a Standards Track RFC to requiring a published RFC of any type. There are two reasons for relaxing the requirement:

- There are some algorithms that are useful that may not be able to be in a Standards Track RFC. For any number of reasons, an algorithm might not have been evaluated thoroughly enough to be able to be put on the Standards Track. Another example is that the algorithm might have unclear intellectual property rights that prevents the algorithm from being put on the Standards Track.

- Although the size of the registry is restricted (about 250 entries), new algorithms are proposed infrequently. It could easily be many decades before there is any reason to consider restricting the registry again.

Some developers will care about the standards level of the RFCs that are in the registry. The registry should be updated to reflect the current standards level of each algorithm listed.

To address concerns about the registry eventually filling up, the IETF should re-evaluate the requirements for entry into this registry when approximately 120 of the registry entries have been assigned. That evaluation may lead to tighter restrictions or a new mechanism for extending the size of the registry. In order to make this evaluation more likely, IANA is requested to mark about half of the currently-available entries as "Reserved" in order to make the timing for that re-evaluation more apparent.

The private-use values, 253 and 254, are still useful for developers who want to test, in private, algorithms for which there is no RFC. This document does not change the semantics of those two values.

3. Expectations For Implementations

It is important to note that, according to RFC 4034, DNSSEC implementations are not expected to include all of the algorithms listed in the IANA registry; in fact, RFC 4034 and the IANA registry list an algorithm that implementations should not include. This document does nothing to change the expectation that there will be items listed in the IANA registry that need not be (and in some cases, should not be) included in all implementations.

There are many reasons why a DNSSEC implementation might not include one or more of the algorithms listed, even those on the Standards Track. In order to be compliant with the RFC 4034, an implementation only needs to implement the algorithms listed as mandatory to implement in that standard, or updates to that standard. This document does nothing to change the list of mandatory to implement algorithms in RFC 4034. This document does not change the requirements for when an algorithm becomes mandatory to implement. Such requirements should come in a separate, focused document.

It should be noted that the order of algorithms in the IANA registry does not signify or imply cryptographic strength or preference.

4. IANA Considerations

This document updates allocation requirements for unassigned values in the "Domain Name System Security (DNSSEC) Algorithm Numbers" registry located at http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml, in the sub-registry titled "DNS Security Algorithm Numbers". The registration procedure for values that are assigned after this document is published is "RFC Required".

IANA is requested to mark values 123 through 251 as "Reserved". The registry should note that this reservation is made in [[THIS RFC]]] so that when most of the unreserved values are taken, the future IANA and users will have an easy pointer to where the reservation originated and its purpose.

IANA is requested to add a textual notation to the "References" column in the registry that gives the current standards status for each RFC that is listed in the registry.

5. Security Considerations

An algorithm described in an RFC that is not on the Standards Track may have weaker security than one that is on the Standards Track; in fact, that may be the reason that the algorithm was not allowed on Standards Track. Note, however, that not being on the Standards Track does not necessarily mean that an algorithm is weaker. Conversely, algorithms that are on the Standards Track should not necessarily be considered better than algorithms that are not on the Standards Track. There are other reasons (such as intellectual property concerns) that can keep algorithms that are widely considered to be strong off of Standards Track.

6. References

6.1. Normative References

[RFC2535] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

[RFC3755] Weiler, S., "Legacy Resolver Compatibility for Delegation Signer (DS)", RFC 3755, May 2004.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

6.2. Informative References

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

Appendix A. Experimental and Documentation Values

During the early discussion of this document, it was proposed that maybe there should be a small number of values reserved for "experimental" purposes. This proposal was not included in this document because of the long history in the IETF of experimental

values that became permanent. That is, a developer would release (maybe "experimentally") a version of software that had the experimental value associated with a particular extension, competitors would code their systems to test interoperability, and then no one wanted to change the values in their software to the "real" value that was later assigned.

There was also a proposal that IANA should reserve two values to be used in documentation only, similar to the way that "example.com" has been reserved as a domain name. That proposal was also not included in this document because all values need to be associated with some algorithm, and there is no problem with having examples that point to commonly-deployed algorithms.

Appendix B. Change History

This section is to be removed before publication as an RFC.

B.1. Differences between draft-hoffman-dnssec-alg-allocation-00 and -01

A few editorial nits that really should have been caught in the -00.

Added the section on "Expectations For Implementations" to clarify that this document is not changing any such expectations or updating that part of RFC 4034.

B.2. Differences between draft-hoffman-dnssec-alg-allocation-01 and draft-ietf-dnsext-dnssec-alg-allocation-00

First WG draft.

Clarified the intent of the document in the Abstract by adding "It does not change the list of algorithms that are recommended or required for DNSSEC implementations".

Added to Section 3: "It should be noted that the order of algorithms in the IANA registry does not signify or imply cryptographic strength or preference."

B.3. Differences between draft-ietf-dnsext-dnssec-alg-allocation-00 and draft-ietf-dnsext-dnssec-alg-allocation-01

Various editorial changes and clarifications that came during WG LC.

Asked IANA to mark values 123 through 250 as "Reserved".

In the expectations for implementers, added "This document does not change the requirements for when an algorithm because mandatory to implement. Such requirements should come in a separate, focused document."

B.4. Differences between draft-ietf-dnsext-dnssec-alg-allocation-01 and draft-ietf-dnsext-dnssec-alg-allocation-02

Reworded the first bullet in Section 2 to remove "government".

B.5. Differences between draft-ietf-dnsext-dnssec-alg-allocation-02 and draft-ietf-dnsext-dnssec-alg-allocation-03

Changed "SHOULD" to "should" in section 2.

In section 4, changed the range of "resevered" codes from "123 through 250" to "123 through 251".

Added to the IANA Considerations: "The registry should note that this reservation is made in [[THIS RFC]]] so that when most of the unreserved values are taken, the future IANA and users will have an easy pointer to where the reservation originated and its purpose."

Author's Address

Paul Hoffman
VPN Consortium

Email: paul.hoffman@vpnc.org