Network Working Group
Internet-Draft
Updates: 2535, 3755, 4034
(if approved)
Intended status: Standards Track
Expires: February 28, 2010

P. Hoffman
VPN Consortium

August 27, 2009

Cryptographic Algorithm Identifier Allocation for DNSSEC
draft-hoffman-dnssec-alg-allocation-01

Status of this Memo

Copyright Notice

Abstract

This document specifies how DNSSEC cryptographic algorithm identifiers in the IANA registries are allocated. It changes the rule from "standard required" to "RFC required".

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 Standards Track as defined in [RFC2026]. The rule from RFC 2535 is repeated in [RFC3755] and [RFC4034].

RFC 2535 allows algorithms that are not on 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 rule for registration from requiring a Standards Track RFC to requiring a published RFC of any type. There are two reasons for relaxing the rule:

- There are some algorithms that are useful that may not be able to be in a Standards Track RFC. For example, an algorithm might be sponsored by a government and use cryptography that has not been evaluated thoroughly enough to be able to be put on Standards Track. Another example is that the algorithm might have an unclear intellectual property rights situation, and that prevents the algorithm from being put on Standards Track.

- Although the size of the registry is quite restricted (about 250 entries), new algorithms are proposed relatively rarely. 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 reflect the current standards level of each algorithm listed.

Because the size of the registry is smaller than many IETF registries, and because some members of the DNS community have expressed concern about the registry eventually filling up, the IETF should re-evaluate the requirements for entry into this registry when the registry is about half full. That evaluation may lead to tighter restrictions or a new mechanism for essentially extending the size of the registry.

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 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 the that standard, or updates to that standard. This document does nothing to change the list of mandatory to implement algorithms in RFC 4034.

4. IANA Considerations

This document updates allocation rules 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 were not assigned before this document is published is "RFC Required".

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 Standards Track may have weaker security than one that is on standards track; in fact, that may be the reason that the algorithm was not allowed on Standards Track. Note, however, that not being on Standards Track does not necessarily mean that an algorithm is weaker. 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 -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.

Author's Address

Paul Hoffman
VPN Consortium

Email: paul.hoffman@vpnc.org