DNS Security (DNSSEC) DNSKEY Algorithm IANA Registry Updates
draft-arends-dnsop-dnssec-algorithm-update-00

Abstract

The DNS Security Extensions (DNSSEC) require the use of cryptographic
algorithm suites for generating digital signatures and cryptographic
hashes over DNS data. The algorithms specified for use with DNSSEC
are reflected in IANA registries. This document updates some entries
in these registries. The main reason for these updates is to retire
the use of SHA1.

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 http://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 September 13, 2017.

Copyright Notice

Copyright (c) 2017 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
(http://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
Internet-Draft          DNSSEC Algorithm Updates              March 2017

1. Introduction

The Domain Name System (DNS) Security Extensions (DNSSEC, defined by [RFC4033], [RFC4034], [RFC4035], [RFC4509], [RFC5155], and [RFC5702]) use digital signatures over DNS data to provide source authentication and integrity protection. DNSSEC uses IANA registries to list codes for digital signature algorithms and hash functions.

This document updates a set of entries in the IANA registries titled "DNS Security (DNSSEC) Algorithm Numbers" and "Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms".

1.1. Reserved Words

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. The DNS Security Algorithm Implementation Status Lists

2.1. Status Definitions

Must Implement: The algorithm MUST be implemented to interoperate with other implementations of this specification.
Internet-Draft          DNSSEC Algorithm Updates              March 2017

Must Not Implement: The algorithm MUST NOT be implemented. An algorithm with this status has known weaknesses.

Recommended to Implement: The algorithm SHOULD be implemented. Utility and interoperability with other implementations will be improved when an algorithm with this status is implemented, though there might be occasions where it is reasonable not to implement the algorithm. An implementer must understand and weigh the full implications of choosing not to implement this particular algorithm.

Optional: The algorithm MAY be implemented, but all implementations MUST be prepared to interoperate with implementations that do or do not implement this algorithm.

2.2. Algorithm Implementation Status Assignment Rationale

RSASHA1 had an implementation status of "Must Implement", consistent with [RFC4034]. The status of RSASHA1 is set to "Recommended to Implement" consistent with RSASHA1-NSEC3-SHA1. The shift from "Must Implement" to "Recommended to Implement" is due to a perceived weakness in SHA1.

The status of RSASHA256 is set to "Must Implement" as major deployments, such as the root zone [RZDPS], use these algorithms. It is believed that RSA/SHA-256 or RSA/SHA-512 algorithms will replace older algorithms (e.g., RSA/SHA-1) that have a perceived weakness.

All other algorithms used in DNSSEC specified without an implementation status are currently set to "Optional".

2.3. DNSSEC Implementation Status Table

The DNSSEC algorithm implementation status table is listed below. Only the algorithms already specified for use with DNSSEC at the time of writing are listed.

<table>
<thead>
<tr>
<th>Must Implement</th>
<th>Must Not Implement</th>
<th>Recommended</th>
<th>Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSASHA256</td>
<td>RSAMD5</td>
<td>RSASHA1</td>
<td>Any registered algorithm not listed in this table</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RSASHA1-NSEC3-SHA1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RSASHA512</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ECDSAP256SHA256</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ECDSAP384SHA384</td>
<td></td>
</tr>
</tbody>
</table>
This table does not list the Reserved values in the IANA registry table or the values for INDIRECT (252), PRIVATE (253), and PRIVATEOID (254). These values may relate to more than one algorithm and are therefore up to the implementer’s discretion. As noted, any algorithm not listed in the table is "Optional".

2.4. Specifying New Algorithms and Updating the Status of Existing Entries

[RFC6014] establishes a parallel procedure for adding a registry entry for a new algorithm other than a standards track document. Because any algorithm not listed in the foregoing table is "Optional", algorithms entered into the registry using the [RFC6014] procedure are automatically "Optional".

It has turned out to be useful for implementations to refer to a single document that specifies the implementation status of every algorithm. Accordingly, when a new algorithm is to be registered with a status other than "Optional", this document shall be made obsolete by a new document that adds the new algorithm to the table in Section 2.3. Similarly, if the status of any algorithm in the table in Section 2.3 changes, a new document shall make this document obsolete; that document shall include a replacement of the table in Section 2.3. This way, the goal of having one authoritative document to specify all the status values is achieved.

This document cannot be updated, only made obsolete and replaced by a successor document.

3. IANA Considerations

This document lists the implementation status of cryptographic algorithms used with DNSSEC. These algorithms are maintained in an IANA registry at <http://www.iana.org/assignments/dns-sec-alg-numbers>. Because this document establishes the implementation status of every algorithm, it has been listed as a reference for the registry itself.

4. Security Considerations

This document lists, and in some cases assigns, the implementation status of cryptographic algorithms used with DNSSEC. It is not meant to be a discussion on algorithm superiority.

Since the status of two algorithms have changed, it is important to consider the long term effect of these changes in implementations.
An implementation may have provided a default algorithm to use when generating a DNSKEY. An implementation may select a default algorithm to sign DNSSEC records. It is recommended that implementations that provide a default algorithm use an algorithm with the status "Must Implement".

5. References

5.1. Normative References


5.2. Informative References


Authors’ Addresses

Roy Arends
ICANN

Email: roy.arends@icann.org

Jakob Schlyter
Kirei AB

Email: jakob@kirei.se

Matt Larson
ICANN

Email: matt.larson@icann.org