DNS Security (DNSSEC) DNSKEY IANA Registry Algorithm Status Addition
draft-ietf-dnsext-dnssec-registry-fixes-04

Abstract

The DNS Security Extensions (DNSSEC) has an IANA registry to allocate
 cryptographic algorithm suites for use in generating digital
 signatures over DNS data. Newly introduced cryptographic algorithms
to DNSSEC mean implementors need to know which algorithms need to be
 implemented, which are optional, and which are obsolete. This
document adds a column to the IANA registry table for Domain Name
System Security (DNSSEC) Algorithm Numbers which lists their current
status for use.

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

This Internet-Draft will expire on November 18, 2010.

Copyright Notice

Copyright (c) 2010 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 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 BSD License.

Table of Contents

1. Introduction .............................................. 3
   1.1. Requirements Language ................................ 3

2. DNS Security Algorithm Number Subregistry Fixes .......... 3
   2.1. Individual Fixes ..................................... 4
   2.2. Updated Registry Snapshot .............................. 5

3. IANA Considerations ....................................... 6

4. Security Considerations .................................... 6

5. References ................................................. 6
   5.1. Normative References .................................. 6
   5.2. Informative References ................................. 7
1. Introduction

The Domain Name System (DNS) Security Extensions (DNSSEC) [RFC4033], [RFC4034], and [RFC4035] uses digital signatures over DNS data to provide source authentication and integrity protection. DNSSEC uses an IANA registry to allocate codes for digital signature algorithms (consisting of a cryptographic algorithm and one-way hash function). Certain digital signature algorithms are considered MANDATORY to implement for interoperability while others listed in this registry are listed as OPTIONAL or OBSOLETE.

The original list of algorithm status is found in [RFC4034]. Other DNSSEC documents have added new algorithms or changed the status of algorithms in the registry. However, implementors must read through all the documents in order to discover which algorithms are mandatory to implement and which are optional or no longer used.

This document requests a column to be added to the IANA registry for Domain Name System Security (DNSSEC) Algorithm Numbers. This column will list the current status of each digital signature algorithm in the registry.

The key words "MANDATORY", "DISCRETIONARY", "OBSOLETE", "DISCOURAGED", "ENCOURAGED" and "RESERVED" in this document are to be interpreted as described in [I-D.ogud-iana-protocol-maintenance-words]

1.1. Requirements Language

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. DNS Security Algorithm Number Subregistry Fixes

The DNS Security Algorithm Number subregistry (part of the Domain Name System (DNS) Security Number registry) will be modified to include a new column. This column will contain the current implementation requirements of the given algorithm. This document does not make any changes to any other column in the registry table.

There are additional fixes to entries that are described in sub-section 2.1. The overall new registry table is in sub-section 2.2. The values for the status were obtained from [RFC4034] with updates for algorithms specified after the original DNSSEC specification. The status of algorithms marked OPTIONAL in [RFC4034] are changed to DISCRETIONARY as defined in [I-D.ogud-iana-protocol-maintenance-words]. The status of algorithms
marked NOT RECOMMENDED in [RFC4034] are changed to OBSOLETE as defined in [I-D.ogud-iana-protocol-maintenance-words].

2.1. Individual Fixes

This document changes three entries in the Domain Name System Security (DNSSEC) Algorithm Registry. They are:

The description for assignment number 4 is changed to "Reserved until 2020".

The description for assignment number 9 is changed to "Reserved until 2020".

The description for assignment number 11 is changed to "Reserved until 2020".

Registry entries 13-251 remains Unassigned.

The status of RSASHA1-NSEC3-SHA1 and DSA-NSEC3-SHA1 are both set to DISCRETIONARY. The status of RSA/SHA-256 and RSA/SHA-512 are set to ENCOURAGED as it is believed that these algorithms will replace older algorithms (e.g. RSA/SHA-1) that have a perceived weakness in their hash algorithm (SHA-1).
### 2.2. Updated Registry Snapshot

As of the current time, the DNS Security Algorithm Number subregistry would look like the following:

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
<th>Zone</th>
<th>Trans</th>
<th>Mnem.</th>
<th>Sign</th>
<th>Sign</th>
<th>Status</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Reserved</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>RSA/MD5</td>
<td></td>
<td></td>
<td>RSAMD5</td>
<td>N</td>
<td>Y</td>
<td>OBSOLETE</td>
<td>[RFC4034], [RFC3110]</td>
</tr>
<tr>
<td>2</td>
<td>Diffie-Hellman</td>
<td></td>
<td></td>
<td>DH</td>
<td>N</td>
<td>Y</td>
<td>DISCRETIONARY</td>
<td>[RFC2539]</td>
</tr>
<tr>
<td>3</td>
<td>DSA/SHA-1</td>
<td></td>
<td></td>
<td>DSASHA1</td>
<td>Y</td>
<td>Y</td>
<td>DISCRETIONARY</td>
<td>[RFC2536], [RFC4034], FIPS 186-3, FIPS 180-3</td>
</tr>
<tr>
<td>4</td>
<td>Reserved until 2020</td>
<td>ECC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>RSA/SHA-1</td>
<td></td>
<td></td>
<td>RSASHA1</td>
<td>Y</td>
<td>Y</td>
<td>MANDATORY</td>
<td>[RFC4034]</td>
</tr>
<tr>
<td>6</td>
<td>DSA-NSEC3-SHA1</td>
<td>DSA-NSEC3-SHA1</td>
<td></td>
<td>DSA-NSEC3-SHA1</td>
<td>Y</td>
<td>Y</td>
<td>DISCRETIONARY</td>
<td>[RFC5155]</td>
</tr>
<tr>
<td>7</td>
<td>RSASHA1-NSEC3-SHA1</td>
<td>RSASHA1-NSEC3-SHA1</td>
<td></td>
<td>RSASHA1-NSEC3-SHA1</td>
<td>Y</td>
<td>Y</td>
<td>DISCRETIONARY</td>
<td>[RFC5155]</td>
</tr>
<tr>
<td>8</td>
<td>RSA/SHA-256</td>
<td></td>
<td></td>
<td>RSASHA256</td>
<td>Y</td>
<td>*</td>
<td>ENCOURAGED</td>
<td>[RFC5702]</td>
</tr>
<tr>
<td>9</td>
<td>Reserved until 2020</td>
<td>RSA/SHA-512</td>
<td></td>
<td>RSASHA512</td>
<td>Y</td>
<td>*</td>
<td>ENCOURAGED</td>
<td>[RFC5702]</td>
</tr>
<tr>
<td>10</td>
<td>Reserved until 2020</td>
<td>GOST R 34.10-2001</td>
<td></td>
<td>GOST-ECC</td>
<td>Y</td>
<td>*</td>
<td>DISCRETIONARY</td>
<td>[RFC5702]</td>
</tr>
<tr>
<td>12</td>
<td>GOST R 34.10-2001</td>
<td>GOST-ECC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13-251</td>
<td>Unassigned</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>252</td>
<td>Reserved for indirect keys</td>
<td>INDIRECT</td>
<td></td>
<td></td>
<td>N</td>
<td>N</td>
<td>DISCRETIONARY</td>
<td>[RFC4034]</td>
</tr>
<tr>
<td>253</td>
<td>Private algorithm</td>
<td>PRIVATE</td>
<td></td>
<td></td>
<td>Y</td>
<td>Y</td>
<td>DISCRETIONARY</td>
<td>[RFC4034]</td>
</tr>
<tr>
<td>254</td>
<td>Private algorithm OID</td>
<td>PRIVATEOID</td>
<td></td>
<td></td>
<td>Y</td>
<td>Y</td>
<td>DISCRETIONARY</td>
<td>[RFC4034]</td>
</tr>
<tr>
<td>255</td>
<td>Reserved</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The requirement status for all new algorithms will be DISCRETIONARY unless a Standards Track document indicates otherwise (possibly including the Standards Track document defining the algorithm). Only a Standards Track document may make an algorithm ENCOURAGED or MANDATORY or remove the MANDATORY or ENCOURAGED designation (to DISCOURAGED or OBSOLETE for example).
3. IANA Considerations

This document consists entirely of DNS IANA Considerations and includes the following changes detailed in Section 2.1:

The description of assignment 4 is changed from "Reserved for ECC" to "Reserved until 2020".

The description of assignment 9 is changed from "Unassigned" to "Reserved until 2020".

The description for assignment number 11 is changed from "Unassigned" to "Reserved until 2020".

Registery entries 13-251 remains Unassigned.

The references for current algorithms in the table in Section 2.2 have been updated to remove obsolete RFC’s and replaced with the current reference.

The references to FIPS 180 and FIPS 186 have been updated (to FIPS 180-3 and FIPS 186-3 respectively) to reflect the latest versions. These revisions are maintenance updates and the relevant content of the FIPS documents have not changed.

The new table is in Section 2.2. The Domain Name System (DNS) Security Algorithm Number registry is available at http://www.iana.org/assignments/dns-sec-alg-numbers/
dns-sec-alg-numbers.xhtml.

4. Security Considerations

This document seeks to add a status column to an existing IANA registry. It is not meant to be a discussion on algorithm superiority. No new security considerations are raised in this document.

5. References

5.1. Normative References

(work in progress),
November 2009.


5.2. Informative References


fips186-3/
fips_186-3.pdf>.


Author’s Address

Scott Rose
NIST
100 Bureau Dr.
Gaithersburg, MD  20899
USA

Phone: +1-301-975-8439
EMail: scottr.nist@gmail.com