DNS Extensions Working Group	S. Rose
Internet-Draft	NIST
Updates: 2536, 2539, 3110, 4034, 4398, 5155, 5702, 5933 (if approved)	May 26, 2011
Intended status: Standards Track	
Expires: November 27, 2011	

Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm IANA Registry
draft-ietf-dnsext-dnssec-registry-fixes-08

Abstract

The DNS Security Extensions (DNSSEC) requires the use of cryptographic algorithm suites for generating digital signatures over DNS data. There is currently an IANA registry for these algorithms that is incomplete in that it lacks the implementation status of each algorithm. This document provides an applicability statement on algorithm implementation compliance status for DNSSEC implementations. This status is to measure compliance to this RFC only. This document replaces that registry table with a new IANA registry table for Domain Name System Security (DNSSEC) Algorithm Numbers that lists (or assigns) each algorithm's status based on the current reference.

Status of this Memo

Copyright Notice

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

The Domain Name System (DNS) Security Extensions (DNSSEC) [RFC4033], [RFC4034], [RFC4035], [RFC4509], [RFC5155], and [RFC5702] uses digital signatures over DNS data to provide source authentication and integrity protection. DNSSEC uses an IANA registry to list codes for digital signature algorithms (consisting of a cryptographic algorithm and one-way hash function).

The original list of algorithm status is found in [RFC4034]. Other DNSSEC RFC's have added new algorithms or changed the status of algorithms in the registry. However, implementers must read through all the documents in order to discover which algorithms are considered wise to implement, which are not, and which algorithms may become widely used in the future. This document replaces the original list with a new table that includes the current compliance status for certain algorithms.

This compliance status indication is only to be considered for implementation, not deployment or operations. Operators are free to deploy any digital signature algorithm available in implementations or algorithms chosen by local security policies. This status is to measure compliance to this RFC only.

This document replaces the current IANA registry for Domain Name System Security (DNSSEC) Algorithm Numbers with a newly defined registry

table. This new table (Section 2.2 below) contains a column that will list the current compliance status of each digital signature algorithm in the registry at the time of writing and assigns status for some algorithms used with DNSSEC that did not have an identified status in their specification. This document updates the following: [RFC2536], [RFC2539], [RFC3110], [RFC4034], [RFC4398], [RFC5155], [RFC5702], and [RFC5933].

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. The DNS Security Algorithm Number Sub-registry

The DNS Security Algorithm Number sub-registry (part of the Domain Name System (DNS) Security Number registry) will be replaced with the table below. This table is based on the existing DNS Security Algorithm Number sub-registry and adds a column that contains the current implementation status of the given algorithm.
There are additional differences 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 compliance status were obtained from [RFC4034] with updates for algorithms specified after the original DNSSEC specification. If no status was listed in the original specification, this document assigns one.

2.1. Updates and Additions

This document updates 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 is set to RECOMMENDED TO IMPLEMENT. This is due to the fact that RSA/SHA-1 is a MUST IMPLEMENT. The status of RSA/SHA-256 and RSA/SHA-512 are also set to RECOMMENDED TO IMPLEMENT as it is believed that these algorithms will replace an older algorithm (e.g. RSA/SHA-1) that have a perceived weakness in its hash algorithm (SHA-1).

2.2. Domain Name System (DNS) Security Algorithm Number Registry Table

The Domain Name System (DNS) Security Algorithm Number registry is hereby specified as follows below. The new column is titled "Compliance

to RFC TBD" (where TBD will change when published) as the IANA Registry table is not normative. The IANA registry table is only a reflection of the RFC, which is normative.

Number	Description	Mnemonic	Zone Sign	Trans-action Sign	Compliance to RFC TBD1	Reference
0	Reserved					[RFC4398]
1	RSA/MD5	RSAMD5	N	Y	MUST NOT IMPLEMENT	[RFC2537]
2	Diffie-Hellman	DH	N	Y		[RFC2539]
3	DSA/SHA-1	DSASHA1	Y	Y		[RFC2536]
4	Reserved until 2020					
5	RSA/SHA-1	RSASHA1	Y	Y	MUST IMPLEMENT	[RFC3110]
6	DSA-NSEC3-SHA1	DSA-NSEC3-SHA1	Y	Y		[RFC5155]
7	RSASHA1-NSEC3-SHA1	RSASHA1-NSEC3-SHA1	Y	Y	RECOMMENDED TO IMPLEMENT	[RFC5155]
8	RSA/SHA-256	RSASHA256	Y	*	RECOMMENDED TO IMPLEMENT	[RFC5702]
9	Reserved until 2020					
10	RSA/SHA-512	RSASHA512	Y	*	RECOMMENDED TO IMPLEMENT	[RFC5702]
11	Reserved until 2020					
12	GOST R 34.10-2001	GOST-ECC	Y	*		[RFC5933]
13-251	Unassigned					
252	Reserved for Indirect keys	INDIRECT	N	N		[RFC4034]
253	private algorithm	PRIVATE	Y	Y		[RFC4034]
254	private algorithm OID	PRIVATEOID	Y	Y		[RFC4034]
255	Reserved					

Table rows where the compliance column is not filled in are left to the discretion of implementers. Their implementation (or lack thereof) therefore cannot be included when judging compliance to this document.

2.3. Specifying New Algorithms and Updating Status of Existing Entries

[RFC6014] establishes a parallel procedure for adding a registry entry for a new algorithm other than a standards track document. Algorithms

entered into the registry using that procedure do not have a listed compliance status. Specifications that follow this path do not need to obsolete or update this document.
Adding a newly specified algorithm to the registry with a compliance status SHALL entail obsolescing this document and replacing the registry table (with the new algorithm entry). Altering the status column value of any existing algorithm in the registry SHALL entail obsoleting this document and replacing the registry table.
This document cannot be updated, only made obsolete and replaced by a successor document.

3. IANA Considerations

This document replaces the Domain Name System (DNS) Security Algorithm Numbers registry. The new registry table is in Section 2.2. In the column "Compliance to RFC TBD", "RFC TBD" should be changed to the official RFC when published.
The original Domain Name System (DNS) Security Algorithm Number registry is available at http://www.iana.org/assignments/dns-sec-alg-numbers.

4. Security Considerations

This document replaces the Domain Name System (DNS) Security Algorithm Numbers registry. It is not meant to be a discussion on algorithm superiority. No new security considerations are raised in this document.

5. References

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[RFC2536]	Eastlake, D.E., "DSA KEYs and SIGs in the Domain Name System (DNS)", RFC 2536, March 1999.
[RFC2537]	Eastlake, D.E., "RSA/MD5 KEYs and SIGs in the Domain Name System (DNS)", RFC 2537, March 1999.
[RFC2539]	Eastlake, D.E., "Storage of Diffie-Hellman Keys in the Domain Name System (DNS)", RFC 2539, March 1999.
[RFC3110]	Eastlake, D., "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)", RFC 3110, May 2001.
[RFC4033]	Arends, R., Austein, R., Larson, M., Massey, D. and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.
[RFC4034]	Arends, R., Austein, R., Larson, M., Massey, D. and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.
[RFC4035]	Arends, R., Austein, R., Larson, M., Massey, D. and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC4398]	Josefsson, S., "Storing Certificates in the Domain Name System (DNS)", RFC 4398, March 2006.
[RFC4509]	Hardaker, W., "Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)", RFC 4509, May 2006.
[RFC5155]	Laurie, B., Sisson, G., Arends, R. and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, March 2008.
[RFC5702]	Jansen, J., "Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC", RFC 5702, October 2009.
[RFC5933]	Dolmatov, V., Chuprina, A. and I. Ustinov, "Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC", RFC 5933, July 2010.
[RFC6014]	Hoffman, P., "Cryptographic Algorithm Identifier Allocation for DNSSEC", RFC 6014, November 2010.

Author's Address

Scott Rose Rose NIST 100 Bureau Dr. Gaithersburg, MD 20899 USA
Phone: +1-301-975-8439 EMail: scottr.nist@gmail.com