DNS Extensions Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 21, 2012

S. Rose
NIST

November 18, 2011

DNS Security (DNSSEC) DNSKEY Algorithm IANA Registry Updates
draft-srose-dnssec-registry-update-00

Abstract

The DNS Security Extensions (DNSSEC) requires the use of cryptographic algorithm suites for generating digital signatures over DNS data. The algorithms specified for use with DNSSEC are reflected in an IANA maintained registry. This document presents a set of changes for some entries of the registry and presents a new registry table.

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 May 21, 2012.

Copyright Notice

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).

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 collection of changes to selected entries originally set aside for future algorithm specification that did not occur. These entries are changed to "Reserved" to avoid potential conflicts with older implementations. This document also brings the list of references for entries up to date.

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. There are additional differences to entries that are described in sub-section 2.1 and the overall new registry table is in sub-section 2.2.

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".

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

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

The above values are changed to "Reserved" because they were placeholders for algorithms that were not fully specified for use with DNSSEC. Older implementations may still have these algorithm codes assigned, so these codes are reserved to prevent potential incompatibilities.

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.

Number	Description	Mnemonic	Zone Sign	Trans-action Sign	Reference
0	Reserved				[RFC4034] [RFC4398]
1	RSA/MD5	RSAMD5	N	Y	[RFC3110]
2	Diffie-Hellman	DH	N	Y	[RFC2539]
3	DSA/SHA-1	DSASHA1	Y	Y	[RFC2536]
4	Reserved				
5	RSA/SHA-1	RSASHA1	Y	Y	[RFC3110]
6	DSA-NSEC3-SHA1	DSA-NSEC3-SHA1	Y	Y	[RFC5155]
7	RSASHA1-NSEC3-SHA1	RSASHA1-NSEC3-SHA1	Y	Y	[RFC5155]
8	RSA/SHA-256	RSASHA256	Y	*	[RFC5702]
9	Reserved				
10	RSA/SHA-512	RSASHA512	Y	*	[RFC5702]
11	Reserved				

12	GOST R 34.10-2001	GOST-ECC	Y	*	[RFC5933]
13-122	Unassigned				
123-251	Reserved				[RFC6014]
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				[RFC4034]

3. IANA Considerations

This document replaces the Domain Name System (DNS) Security Algorithm Numbers registry with new registry table is in Section 2.2. The changes include moving three registry entries to "Reserved" and updating the reference list for entries.

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 with an updated table. It is not meant to be a discussion on algorithm superiority. No new security considerations are raised in this document.

5. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2536] Eastlake, D., "DSA KEYs and SIGs in the Domain Name System (DNS)", RFC 2536, March 1999.

[RFC2539] Eastlake, D., "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
NIST
100 Bureau Dr.

Gaithersburg, MD 20899
USA

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