Internet Engineering Task Force (IETF)
Request for Comments: 6725
Category: Standards Track
ISSN: 2070-1721

S. Rose
NIST

August 2012

DNS Security (DNSSEC) DNSKEY Algorithm IANA Registry Updates

Abstract

The DNS Security Extensions (DNSSEC) require 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.

Status of This Memo

Copyright Notice

Table of Contents

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 an IANA registry to list codes for digital signature algorithms (consisting of an asymmetric cryptographic algorithm and a one-way hash function).

This document updates a set of entries in the IANA registry titled "DNS Security (DNSSEC) Algorithm Numbers". These updated entries are given in Section 2.2 below. This list includes changes to selected entries originally set aside for future algorithm specification that did not occur. These three 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.

There are auxiliary sub-registries related to the DNS Security (DNSSEC) Algorithm Numbers registry that deal with various Diffie-Hellman parameters used with DNSSEC. These registry tables are not altered by this document.

2. The DNS Security Algorithm Numbers Sub-Registry

The DNS Security Algorithm Numbers sub-registry (part of the Domain Name System Security (DNSSEC) Algorithm Numbers registry) contains a set of entries that contain errors. There are additional differences to entries that are described in Section 2.1, and the complete list of changed registry entries is in Section 2.2.

2.1. Updates and Additions

This document updates three entries in the Domain Name System Security (DNSSEC) Algorithm Numbers registry:

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 entries 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. DNS Security Algorithm Numbers Sub-Registry Table

The list of DNS Security Algorithm Numbers sub-registry entry changes is given below. All other existing entries in the sub-registry table are unchanged by this document and are not shown. The other two sub-registries in the Domain Name System Security (DNSSEC) Algorithm Numbers registry (DNS KEY Record Diffie-Hellman Prime Lengths and DNS KEY Record Diffie-Hellman Well-Known Prime/Generator Pairs) are not changed in any way by this document.

Number	Description	Mnemonic	Zone Signing	Trans. Sec.	Reference
0	Reserved				[RFC4034], [RFC4398]
1	RSA/MD5 (deprecated; see 5)	RSAMD5	N	Y	[RFC3110], [RFC4034]
4	Reserved				[RFC6725]
5	RSA/SHA-1	RSASHA1	Y	Y	[RFC3110], [RFC4034]
9	Reserved				[RFC6725]
11	Reserved				[RFC6725]
15-122	Unassigned				
123-251	Reserved				[RFC4034], [RFC6014]
253	private algorithm	PRIVATEDNS	Y	Y	[RFC4034]
254	private algorithm OID	PRIVATEOID	Y	Y	[RFC4034]

3. IANA Considerations

This document updates a set of DNS Security Algorithm Numbers sub-registry entries as given in Section 2.2. The changes include moving three registry entries to "Reserved" and updating the reference list for entries.

4. Security Considerations

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

5. Informative References

[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.

[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