DNS Extensions Working Group
Internet-Draft
Updates: 2536, 2539, 3110, 4034, 4398,
5155, 5702, 5933 (if approved)
Intended status: BCP
Expires: September 27, 2012

S. Rose
NIST

March 26, 2012

Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status
draft-ietf-dnsext-dnssec-algo-imp-status-01

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 recommended implementation status of each algorithm. This document provides an applicability statement on algorithm implementation status for DNSSEC component software. This document lists each algorithm's status based on the current reference. In the case that an algorithm is specified without an implementation status, this document assigns one.

Status of This Memo

Copyright Notice

Table of Contents

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

   2.  The DNS Security Algorithm Implementation Status Lists  . . . .  3
     2.1.  Algorithm Implementation Status Assignement Rationale . . .  3
     2.2.  DNSSEC Implementation Status Table  . . . . . . . . . . . .  4
     2.3.  Specifying New Algorithms and Updating Status of
           Existing Entries  . . . . . . . . . . . . . . . . . . . . .  4

   3.  IANA Considerations . . . . . . . . . . . . . . . . . . . . . .  5

   4.  Security Considerations . . . . . . . . . . . . . . . . . . . .  5

   5.  References  . . . . . . . . . . . . . . . . . . . . . . . . . .  5
     5.1.  Normative References  . . . . . . . . . . . . . . . . . . .  5
     5.2.  Informative References  . . . . . . . . . . . . . . . . . .  6
```

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 includes the current implementation status for certain algorithms.

This implementation 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 document only.

This document updates the following: [RFC2536], [RFC2539], [RFC3110], [RFC4034], [RFC4398], [RFC5155], [RFC5702], and [RFC5933].

1.1. Requirements Language

The key words "MUST", "MUST NOT", "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. Algorithm Implementation Status Assignement Rationale

The status of RSASHA1-NSEC3-SHA1 is set to RECOMMENDED TO IMPLEMENT as major deployments (such as the root zone) use NSEC3 [ROOTDPS]. 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) as well as seen in major deployments.

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

2.2. 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.

MUST IMPLEMENT	MUST NOT IMPLEMENT	RECOMMENDED TO IMPLEMENT	OPTIONAL
RSASHA1	RSAMD5	RSASHA256 RSASHA1-NSEC3-SHA1 RSASHA512	DSASHA1 DH DSA-NSEC3-SHA1 GOST-ECC ECDSAP256SHA256 ECDSAP384SHA384

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. 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 are to be considered OPTIONAL for implementation purposes. Specifications that follow this path do not need to obsolete or update this document.

Adding a newly specified algorithm to the registry with a implementation status other than OPTIONAL SHALL entail obsolescing this document and replacing the table in Section 2.2 (with the new algorithm entry). Altering the status column value of any existing algorithm in the registry SHALL entail obsolescing this document and replacing the table in Section 2.2 above.

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. There are no changes to the registry in this document. However this document asks to be listed as a reference for the entire registry.

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. No new security considerations are raised in this document.

5. References

5.1. 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.

5.2. Informative References

[ROOTDPS] Ljunggren, F., Okubo, T., Lamb, R., and J. Schlyter, "DNSSEC Practice Statement for the Root Zone KSK Operator", DNS ROOTDPS, May 2010, <http://www.root-dnssec.org/wp-content/uploads/2010/06/icann-dps-00.txt>.

Author's Address

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

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