Internet Engineering Task Force (IETF)
Request for Comments: 6944
Updates: 2536, 2539, 3110, 4034, 4398, 5155, 5702, 5933
Category: Standards Track
ISSN: 2070-1721

S. Rose
NIST

April 2013

Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status

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, but there is no record of 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. This document updates RFCs 2536, 2539, 3110, 4034, 4398, 5155, 5702, and 5933.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6944.

Copyright Notice

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 RFCs 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 defines the current implementation status for all registered algorithms. If the status of algorithms changes, this document will be replaced with a new one establishing the new status; see Section 2.4.

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 Implementation Status Lists

2.1. Status Definitions

Must Implement: The algorithm MUST be implemented to interoperate with other implementations of this specification.

Must Not Implement: The algorithm MUST NOT be implemented. An algorithm with this status has known weaknesses.

Recommended to Implement: The algorithm SHOULD be implemented. Utility and interoperability with other implementations will be improved when an algorithm with this status is implemented, though there might be occasions where it is reasonable not to implement the algorithm. An implementer must understand and weigh the full implications of choosing not to implement this particular algorithm.

Optional: The algorithm MAY be implemented, but all implementations MUST be prepared to interoperate with implementations that do or do not implement this algorithm.

2.2. Algorithm Implementation Status Assignment Rationale

RSASHA1 has an implementation status of Must Implement, consistent with [RFC4034]. RSAMD5 has an implementation status of Must Not Implement because of known weaknesses in MD5.

The status of RSASHA1-NSEC3-SHA1 is set to Recommended to Implement as many deployments use NSEC3. The status of RSA/SHA-256 and RSA/SHA-512 are also set to Recommended to Implement as major deployments (such as the root zone) use these algorithms [ROOTDPS]. It is believed that RSA/SHA-256 or RSA/SHA-512 algorithms will replace older algorithms (e.g., RSA/SHA-1) that have a perceived weakness.

Likewise, ECDSA with the two identified curves (ECDSAP256SHA256 and ECDSAP384SHA384) is an algorithm that may see widespread use due to the perceived similar level of security offered with smaller key size compared to the key sizes of algorithms such as RSA. Therefore, ECDSAP256SHA256 and ECDSAP384SHA384 are Recommended to Implement.

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

2.3. 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 ECDSAP256SHA256 ECDSAP384SHA384	Any registered algorithm not listed in this table

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. As noted, any algorithm not listed in the table is Optional. As of this writing, the Optional algorithms are DSASHA1, DH, DSA-NSEC3-SHA1, and GOST-ECC, but in general, anything not explicitly listed is Optional.

2.4. Specifying New Algorithms and Updating the Status of Existing Entries

[RFC6014] establishes a parallel procedure for adding a registry entry for a new algorithm other than a standards track document. Because any algorithm not listed in the foregoing table is Optional, algorithms entered into the registry using the [RFC6014] procedure are automatically Optional.

It has turned out to be useful for implementations to refer to a single document that specifies the implementation status of every algorithm. Accordingly, when a new algorithm is to be registered with a status other than Optional, this document shall be made obsolete by a new document that adds the new algorithm to the table in Section 2.3. Similarly, if the status of any algorithm in the table in Section 2.3 changes, a new document shall make this document obsolete; that document shall include a replacement of the table in Section 2.3. This way, the goal of having one authoritative document to specify all the status values is achieved.

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 at http://www.iana.org/assignments/dns-sec-alg-numbers. Because this document establishes the implementation status of every algorithm, it has been listed as a reference for the registry itself.

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, though prior description of algorithms as NOT RECOMMENDED (see [RFC4034]) has been recast as Must Not Implement.

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