Network Working Group
Internet-Draft
Expires: May 14, 2006

W. Hardaker
Sparta

November 10, 2005

Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs) draft-ietf-dnsext-ds-sha256-00.txt

Status of this Memo

Copyright Notice

Abstract

This document defines the use of the SHA-256 digest type for creating digests of DNSKEY Resource Records (RRs). These digests can then be published in Delegation Signer (DS) resource records (RRs) by a parent zone.

Table of Contents

1. Introduction

The DNSSEC [RFC4033] [RFC4034] [RFC4035] DS RR is published by parent zones to distribute a cryptographic digest of a child's Key Signing Key (KSK) DNSKEY RR. This DS RR is signed using the parent zone's private half of it's DNSKEY and is published in a RRSIG record.

2. Implementing the SHA-256 algorithm for DS record support

This document specifies that the digest type code [XXX: To be assigned by IANA; likely 2] is to be assigned to SHA-256 [SHA256] for use within DS records. The results of the digest algorithm MUST NOT be truncated and the entire 32 byte digest result is to be published in the DS record.

2.1. DS record field values

Using the SHA-256 digest algorithm within a DS record will make use of the following DS-record fields:

Digest type: [XXX: To be assigned by IANA; likely 2]

Digest: A SHA-256 bit digest value calculated by using the following formula ("|" denotes concatenation). The resulting value is not truncated and the entire 32 byte result is to used in the resulting DS record and related calculations.

```
digest = SHA_256(DNSKEY owner name | DNSKEY RDATA)
```

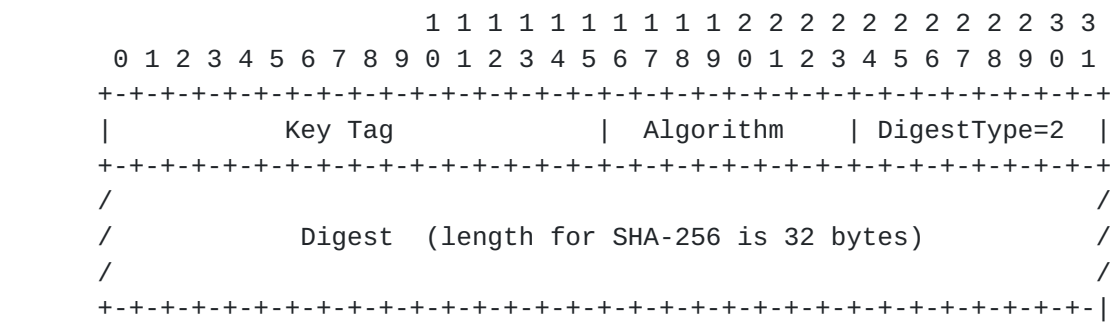
where DNSKEY RDATA is defined by [RFC4034] as:

```
DNSKEY RDATA = Flags | Protocol | Algorithm | Public Key
```

The Key Tag field and Algorithm fields remain unchanged by this document and are specified in the [RFC4034] specification.

2.2. DS Record with SHA-256 Wire Format

The resulting packet format for the resulting DS record will be [XXX: IANA assignment should replace the 2 below]:



3. Implementation Requirements

Implementations MUST support the use of the SHA-256 algorithm in DS RRs.

Implementations that support SHA-256 MUST prefer DS records with SHA-256 (digest type number [XXX: RFC to be assigned by IANA; likely 2]) digests over DS records with SHA-1 (digest type number 1) digests.

4. Deployment Requirements

Deployments SHOULD publish both SHA-1 and SHA-256 based DS records for 2 years from the publication date of this RFC (XXX: RFC Editor: Please insert the calculated date here).

5. IANA Considerations

The Digest Type to be used for supporting SHA-256 within DS records needs to be assigned by IANA. This document requests that the Digest Type value of 2 be assigned to the SHA-256 digest algorithm.

6. Security Considerations

Because of the weaknesses recently discovered within the SHA-1 algorithm, users of DNSSEC are encouraged to deploy the use of SHA-256 as soon as software implementations in use allow for it.

At the time of this publication, the SHA-256 algorithm is considered sufficiently strong for the immediate future. It is considered also considered sufficient for use in DNSSEC DS RRs for the immediate future. However, future published attacks may, of course, weaken the usability of this algorithm within the DS RRs.

7. Acknowledgments

This document is a minor extension to the existing DNSSEC documents and those authors are gratefully appreciated for the hard work that went into the base documents.

8. References

8.1. Normative References

[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.

[SHA256] National Institute of Standards and Technology, "Secure Hash Algorithm. NIST FIPS 180-2", August 2002.

8.2. Informative References

Appendix A. Example

TBD

Author's Address

Wes Hardaker
Sparta
P.O. Box 382
Davis 95617
US

Email: hardaker@tislabs.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.