DNS Extensions working group
Internet-Draft
Expires: June 13, 2008

J. Jansen
NLnet Labs

December 11, 2007

Use of SHA-2 algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC
draft-ietf-dnsext-dnssec-rsasha256-02

Status of this Memo

Copyright Notice

Abstract

This document describes how to produce RSA/SHA-256 and RSA/SHA-512 DNSKEY and RRSIG resource records for use in the Domain Name System Security Extensions (DNSSEC, RFC4033, RFC4034, and RFC4035).

Table of Contents

1. Introduction

The Domain Name System (DNS) is the global hierarchical distributed database for Internet Addressing. The DNS has been extended to use cryptographic keys and digital signatures for the verification of the integrity of its data. RFC4033 [1], RFC4034 [2], and RFC4035 [3] describe these DNS Security Extensions, called DNSSEC.

RFC4034 describes how to store DNSKEY and RRSIG resource records, and specifies a list of cryptographic algorithms to use. This document extends that list with the algorithm RSA/SHA-256 and RSA/SHA-512, and specifies how to store DNSKEY data and how to produce RRSIG resource records with these hash algorithms.

Familiarity with DNSSEC, RSA [7] and the SHA-2 [5] family of algorithms is assumed in this document.

To refer to both SHA-256 and SHA-512, this document will use the name SHA-2. This is done to improve readability. When a part of text is specific for either SHA-256 or SHA-512, their specific names are used. The same goes for RSA/SHA-256 and RSA/SHA-512, which will be grouped using the name RSA/SHA-2.

2. DNSKEY Resource Records

The format of the DNSKEY RR can be found in RFC4034 [2] and RFC3110 [6].

2.1. RSA/SHA-256 DNSKEY Resource Records

RSA public keys for use with RSA/SHA-256 are stored in DNSKEY resource records (RRs) with the algorithm number [TBA].

For use with NSEC3, the algorithm number of RSA/SHA-256 will be [TBA].

2.2. RSA/SHA-512 DNSKEY Resource Records

RSA public keys for use with RSA/SHA-512 are stored in DNSKEY resource records (RRs) with the algorithm number [TBA].

For use with NSEC3, the algorithm number of RSA/SHA-512 will be [TBA].

3. RRSIG Resource Records

The value of the signature field in the RRSIG RR is calculated as follows. The values for the fields that precede the signature data are specified in RFC4034 [2].

hash = SHA-XXX(data)

Where XXX is either 256 or 512, depending on the algorithm used.

signature = (00 | 01 | FF* | 00 | prefix | hash) ** e (mod n)

Where SHA-XXX is the message digest algorithm as specified in FIPS 180 [5], | is concatenation, 00, 01, FF and 00 are fixed octets of corresponding hexadecimal value, "e" is the private exponent of the signing RSA key, and "n" is the public modulus of the signing key. The FF octet MUST be repeated the maximum number of times so that the total length of the signature equals the length of the modulus of the signer's public key ("n"). "data" is the data of the resource record set that is signed, as specified in RFC4034 [2].

The prefix should make the use of standard cryptographic libraries easier. These specifications are taken directly from PKCS #1 v2.1 section 9.2 [4]. The prefixes for the different algorithms are specified below.

3.1. RSA/SHA-256 RRSIG Resource Records

RSA/SHA-256 signatures are stored in the DNS using RRSIG resource records (RRs) with algorithm number [TBA].

The prefix is the ASN.1 BER SHA-256 algorithm designator prefix as specified in PKCS 2.1 [4]:

hex 30 31 30 0d 06 09 60 86 48 01 65 03 04 02 01 05 00 04 20

3.2. RSA/SHA-512 RRSIG Resource Records

RSA/SHA-512 signatures are stored in the DNS using RRSIG resource records (RRs) with algorithm number [TBA].

The prefix is the ASN.1 BER SHA-512 algorithm designator prefix as specified in PKCS 2.1 [4]:

hex 30 51 30 0d 06 09 60 86 48 01 65 03 04 02 03 05 00 04 40

4. Implementation Considerations

DNSSEC aware implementations SHOULD be able to support RRSIG resource records with the RSA/SHA-2 algorithms.

If both RSA/SHA-2 and RSA/SHA-1 RRSIG resource records are available for a certain rrset, with a secure path to their keys, the validator SHOULD ignore the SHA-1 signature. If the RSA/SHA-2 signature does not verify the data, and the RSA/SHA-1 signature does, the validator SHOULD mark the data with the security status from the RSA/SHA-2 signature.

5. IANA Considerations

IANA has not yet assigned an algorithm number for RSA/SHA-256 and RSA/SHA-512.

The algorithm list from RFC4034 Appendix A.1 [2] is extended with the following entries:

Value	Algorithm	[Mnemonic]	Zone Signing	References	Status
[TBA]	RSA/SHA-256	[RSASHA256]	y	[TBA]	OPTIONAL
[TBA]	RSA/SHA-256-NSEC3	[RSASHA256NSEC3]	y	[TBA]	OPTIONAL
[TBA]	RSA/SHA-512	[RSASHA512]	y	[TBA]	OPTIONAL
[TBA]	RSA/SHA-512-NSEC3	[RSASHA512NSEC3]	y	[TBA]	OPTIONAL

6. Security Considerations

6.1. SHA-1 versus SHA-2 Considerations for RRSIG resource records

Users of DNSSEC are encouraged to deploy SHA-2 as soon as software implementations allow for it. SHA-2 is widely believed to be more resilient to attack than SHA-1, and confidence in SHA-1's strength is being eroded by recently-announced attacks. Regardless of whether or not the attacks on SHA-1 will affect DNSSEC, it is believed (at the time of this writing) that SHA-2 is the better choice for use in DNSSEC records.

SHA-2 is considered sufficiently strong for the immediate future, but predictions about future development in cryptography and cryptanalysis are beyond the scope of this document.

6.2. Signature Type Downgrade Attacks

Since each RRset MUST be signed with each algorithm present in the DNSKEY RRset at the zone apex (see [3] Section 2.2), a malicious party cannot filter out the RSA/SHA-2 RRSIG, and force the validator to use the RSA/SHA-1 signature if both are present in the zone. Together with the implementation considerations from Section 4 of this document, this provides resilience against algorithm downgrade attacks, if the validator supports RSA/SHA-2.

7. Acknowledgments

This document is a minor extension to RFC4034 [2]. Also, we try to follow the documents RFC3110 [6] and RFC4509 [8] for consistency. The authors of and contributors to these documents are gratefully acknowledged for their hard work.

The following people provided additional feedback and text: Jaap Akkerhuis, Rob Austein, Miek Gieben, Scott Rose and Wouter Wijngaards.

8. References

8.1. Normative References

[1] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[2] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[3] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[4] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003.

[5] National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-2, August 2002.

[6] Eastlake, D., "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)", RFC 3110, May 2001.

8.2. Informative References

[7] Schneier, B., "Applied Cryptography Second Edition: protocols, algorithms, and source code in C", Wiley and Sons , ISBN 0-471-11709-9, 1996.

[8] Hardaker, W., "Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)", RFC 4509, May 2006.

Author's Address

Jelte Jansen
NLnet Labs
Kruislaan 419
Amsterdam 1098VA
NL

Email: jelte@NLnetLabs.nl
URI: http://www.nlnetlabs.nl/

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).