DNS Extensions working group	J. Jansen	
Internet-Draft	NLnet Labs	
Intended status: Standards Track	December 03, 2008	
Expires: June 6, 2009		

TOC

Use of SHA-2 algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC
draft-ietf-dnsext-dnssec-rsasha256-07

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.
Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as “work in progress.”
The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.
The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.
This Internet-Draft will expire on June 6, 2009.

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, RFC 4033, RFC 4034, and RFC 4035).

Table of Contents

1. Introduction
2. DNSKEY Resource Records
    2.1. RSA/SHA-256 DNSKEY Resource Records
    2.2. RSA/SHA-512 DNSKEY Resource Records
3. RRSIG Resource Records
    3.1. RSA/SHA-256 RRSIG Resource Records
    3.2. RSA/SHA-512 RRSIG Resource Records

4. Deployment Considerations
4.1. Key Sizes
4.2. Signature Sizes
5. Implementation Considerations
5.1. Support for SHA-2 signatures
6. IANA Considerations
7. Security Considerations
7.1. SHA-1 versus SHA-2 Considerations for RRSIG Resource Records
7.2. Signature Type Downgrade Attacks
8. Acknowledgments
9. References
9.1. Normative References
9.2. Informative References
§ Author's Address
§ Intellectual Property and Copyright Statements

---

1. Introduction

TOC

The Domain Name System (DNS) is the global hierarchical distributed database for Internet Naming. The DNS has been extended to use cryptographic keys and digital signatures for the verification of the authenticity and integrity of its data. RFC 4033 [RFC4033] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “DNS Security Introduction and Requirements,” March 2005.), RFC 4034 [RFC4034] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Resource Records for the DNS Security Extensions,” March 2005.), and RFC 4035 [RFC4035] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Protocol Modifications for the DNS Security Extensions,” March 2005.) describe these DNS Security Extensions, called DNSSEC. RFC 4034 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 algorithms 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 and the SHA-2 [FIPS.180-2.2002] (National Institute of Standards and Technology, “Secure Hash Standard,” August 2002.) 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.

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] (Bradner, S.,

"Key words for use in RFCs to Indicate Requirement Levels," March 1997.).

---

2. DNSKEY Resource Records

TOC

The format of the DNSKEY RR can be found in RFC 4034 [RFC4034] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions," March 2005.). RFC 3110 [RFC3110] (Eastlake, D., "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)," May 2001.) describes the use of RSA/SHA-1 for DNSSEC signatures.

2.1. RSA/SHA-256 DNSKEY Resource Records

TOC

RSA public keys for use with RSA/SHA-256 are stored in DNSKEY resource records (RRs) with the algorithm number {TBA1}.
For use with NSEC3 [RFC5155] (Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence," March 2008.), the algorithm number for RSA/SHA-256 will be {TBA2}. The use of a different algorithm number to differentiate between the use of NSEC and NSEC3 is in keeping with the approach adopted in RFC5155.
For interoperability, as in RFC 3110 [RFC3110] (Eastlake, D., "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)," May 2001.), the key size of RSA/SHA-256 keys MUST NOT be less than 512 bits, and MUST NOT be more than 4096 bits.

2.2. RSA/SHA-512 DNSKEY Resource Records

TOC

RSA public keys for use with RSA/SHA-512 are stored in DNSKEY resource records (RRs) with the algorithm number {TBA3}.
For use with NSEC3, the algorithm number for RSA/SHA-512 will be {TBA4}. The use of a different algorithm number to differentiate between the use of NSEC and NSEC3 is in keeping with the approach adopted in RFC5155.
The key size of RSA/SHA-512 keys MUST NOT be less than 1024 bits, and MUST NOT be more than 4096 bits.

TOC

3. RRSIG Resource Records

The value of the signature field in the RRSIG RR follows the RSASSA-PKCS1-v1_5 signature scheme, and is calculated as follows. The values for the RDATA fields that precede the signature data are specified in RFC 4034 [RFC4034] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions," March 2005.).

hash = SHA-XXX(data)

Here XXX is either 256 or 512, depending on the algorithm used, as specified in FIPS PUB 180-2 [FIPS.180-2.2002] (National Institute of Standards and Technology, "Secure Hash Standard," August 2002.), and "data" is the wire format data of the resource record set that is signed, as specified in RFC 4034 [RFC4034] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions," March 2005.).

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

Here "|" 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 exact number of times so that the total length of the concatenated term in parentheses equals the length of the modulus of the signer's public key ("n").

The "prefix" is intended to make the use of standard cryptographic libraries easier. These specifications are taken directly from the specifications of RSASSA-PKCS1-v1_5 in PKCS #1 v2.1 section 8.2 [RFC3447] (Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1," February 2003.), and EMSA-PKCS1-v1_5 encoding in PKCS #1 v2.1 section 9.2 [RFC3447] (Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1," February 2003.). The prefixes for the different algorithms are specified below.

3.1. RSA/SHA-256 RRSIG Resource Records

TOC

RSA/SHA-256 signatures are stored in the DNS using RRSIG resource records (RRs) with algorithm number {TBA1} for use with NSEC, or {TBA2} for use with NSEC3.

The prefix is the ASN.1 DER SHA-256 algorithm designator prefix as specified in PKCS #1 v2.1 [RFC3447] (Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1," February 2003.):

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

TOC

RSA/SHA-512 signatures are stored in the DNS using RRSIG resource records (RRs) with algorithm number {TBA3} for use with NSEC, or {TBA4} for use with NSEC3.
The prefix is the ASN.1 DER SHA-512 algorithm designator prefix as specified in PKCS #1 v2.1 [RFC3447] (Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1," February 2003.):
hex 30 51 30 0d 06 09 60 86 48 01 65 03 04 02 03 05 00 04 40

---

4. Deployment Considerations

TOC

4.1. Key Sizes

TOC

Apart from the restrictions specified in section 2, this document will not specify what size of keys to use. That is an operational issue and depends largely on the environment and intended use. A good starting point for more information would be NIST SP 800-57 [NIST800-57] (Barker, E., Barker, W., Burr, W., Polk, W., and M. Smid, "Recommendations for Key Management," March 2007.).

4.2. Signature Sizes

TOC

In this family of signing algorithms, the size of signatures is related to the size of the key, and not the hashing algorithm used in the signing process. Therefore, RRSIG resource records produced with RSA/SHA256 or RSA/SHA512 will have the same size as those produced with RSA/SHA1, if the keys have the same length.

---

5. Implementation Considerations

TOC

TOC

5.1. Support for SHA-2 signatures

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

---

6. IANA Considerations

TOC

Note to the RFC editor: please remove this paragraph during final editing, and request IANA to update the {TBA} designators.
IANA has assigned DNS Security Algorithm Numbers {TBA1} for RSA/SHA-256 with NSEC, {TBA2} for RSA/SHA-256 with NSEC3, {TBA3} for RSA/SHA-512 with NSEC, and {TBA4} for RSA/SHA-512 with NSEC3.
The algorithm list from RFC 4034 Appendix A.1 [RFC4034] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Resource Records for the DNS Security Extensions,” March 2005.) is extended with the following entries:

Value	Algorithm	Mnemonic	Zone Signing	References
{TBA1}	RSA/SHA-256	RSASHA256	y	{this memo}
{TBA2}	RSA/SHA-256-NSEC3	RSASHA256NSEC3	y	{this memo}
{TBA3}	RSA/SHA-512	RSASHA512	y	{this memo}
{TBA4}	RSA/SHA-512-NSEC3	RSASHA512NSEC3	y	{this memo}

---

7. Security Considerations

TOC

7.1. SHA-1 versus SHA-2 Considerations for RRSIG Resource Records

TOC

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.

The signature scheme RSASSA-PKCS1-v1_5 is chosen to match the one used for RSA/SHA-1 signatures. This should ease implementation of the new hashing algorithms in DNSSEC software.

7.2. Signature Type Downgrade Attacks

TOC

Since each RRSet MUST be signed with each algorithm present in the DNSKEY RRSet at the zone apex (see [RFC4035] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Protocol Modifications for the DNS Security Extensions,” March 2005.) 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. This should provide resilience against algorithm downgrade attacks, if the validator supports RSA/SHA-2.

---

8. Acknowledgments

TOC

This document is a minor extension to RFC 4034 [RFC4034] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Resource Records for the DNS Security Extensions,” March 2005.). Also, we try to follow the documents RFC 3110 [RFC3110] (Eastlake, D., “RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS),” May 2001.) and RFC 4509 [RFC4509] (Hardaker, W., “Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs),” May 2006.) 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, Roy Arends, Rob Austein, Francis Dupont, Miek Gieben, Alfred Hoenes, Paul Hoffman, Peter Koch, Michael St. Johns, Scott Rose and Wouter Wijngaards.

---

9. References

TOC

9.1. Normative References

TOC

[FIPS. 180-2.2002]	National Institute of Standards and Technology, “Secure Hash Standard,” FIPS PUB 180-2, August 2002.
[RFC2119]	

	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119, March 1997 (TXT).
[RFC3110]	Eastlake, D., "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)," RFC 3110, May 2001 (TXT).
[RFC4033]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements," RFC 4033, March 2005 (TXT).
[RFC4034]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions," RFC 4034, March 2005 (TXT).
[RFC4035]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions," RFC 4035, March 2005 (TXT).

9.2. Informative References

TOC

[NIST800-57]	Barker, E., Barker, W., Burr, W., Polk, W., and M. Smid, "Recommendations for Key Management," NIST SP 800-57, March 2007.
[RFC3447]	Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1," RFC 3447, February 2003 (TXT).
[RFC4509]	Hardaker, W., "Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)," RFC 4509, May 2006 (TXT).
[RFC5155]	Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence," RFC 5155, March 2008 (TXT).

Author's Address

TOC

	Jelte Jansen
	NLnet Labs
	Kruislaan 419
	Amsterdam 1098VA
	NL
Email:	jelte@NLnetLabs.nl
URI:	http://www.nlnetlabs.nl/

Full Copyright Statement

TOC

Copyright © The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.
This document and the information contained herein are provided on an “AS IS” basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.
Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.
The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.