DNS Extensions working group J. Jansen
Internet-Draft NLnet Labs
Intended status: Standards Track February 27, 2009
Expires: August 31, 2009

Use of SHA-2 algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC

draft-ietf-dnsext-dnssec-rsasha256-11

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

Table of Contents

1. Introduction

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], RFC 4034 [RFC4034], and RFC 4035 [RFC4035] 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.180-3.2008] 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 term "SHA-2" is not officially defined, but is usually used to refer to the collection of the algorithms SHA-224, SHA-256, SHA-384 and SHA-512. Since SHA-224 and SHA-384 are not used in DNSSEC, SHA-2 will only refer to SHA-256 and SHA-512 in this document.

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. DNSKEY Resource Records

The format of the DNSKEY RR can be found in RFC 4034 [RFC4034]. RFC 3110 [RFC3110] describes the use of RSA/SHA-1 for DNSSEC signatures.

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 {TBA1}.

For interoperability, as in RFC 3110 [RFC3110], 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

RSA public keys for use with RSA/SHA-512 are stored in DNSKEY resource records (RRs) with the algorithm number {TBA2}.

The key size of RSA/SHA-512 keys MUST NOT be less than 1024 bits, and MUST NOT be more than 4096 bits.

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].

hash = SHA-XXX(data)

Here XXX is either 256 or 512, depending on the algorithm used, as specified in FIPS PUB 180-3 [FIPS.180-3.2008], and "data" is the wire format data of the resource record set that is signed, as specified in RFC 4034 [RFC4034].

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], and EMSA-PKCS1-v1_5 encoding in PKCS #1 v2.1 section 9.2 [RFC3447]. 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 {TBA1}.

The prefix is the ASN.1 DER SHA-256 algorithm designator prefix as specified in PKCS #1 v2.1 [RFC3447]:

```
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 {TBA2}.

The prefix is the ASN.1 DER SHA-512 algorithm designator prefix as specified in PKCS #1 v2.1 [RFC3447]:

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

4. Deployment Considerations

4.1. Key Sizes

Apart from the restrictions 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].

4.2. Signature Sizes

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

5.1. Support for SHA-2 signatures

DNSSEC aware implementations SHOULD be able to support RRSIG and DNSKEY resource records created with the RSA/SHA-2 algorithms as defined in this document.

5.2. Support for NSEC3 Denial of Existence

RFC5155 [RFC5155] defines new algorithm identifiers for existing signing algorithms, to indicate that zones signed with these algorithm identifiers use NSEC3 instead of NSEC records to provide denial of existence. That mechanism was chosen to protect implementations predating RFC5155 from encountering resource records they could not know about. This document does not define such algorithm aliases, and support for NSEC3 denial of existence is implicitly signaled with support for one of the algorithms defined in this document.

5.2.1. NSEC3 in Authoritative servers

An authoritative server that does not implement NSEC3 MAY still serve zones that use RSA/SHA2 with NSEC denial of existence.

5.2.2. NSEC3 in Validators

A DNSSEC validator that implements RSA/SHA2 MUST be able to handle both NSEC and NSEC3 [RFC5155] negative answers. If this is not the case, the validator MUST treat a zone signed with RSA/SHA256 or RSA/SHA512 as signed with an unknown algorithm, and thus as insecure.

6. IANA Considerations

This document updates the IANA registry "DNS SECURITY ALGORITHM NUMBERS -- per [RFC4035] " (http://www.iana.org/assignments/dns-sec-alg-numbers). The following entries are added to the registry:

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

7. Security Considerations

7.1. 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.

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

Since each RRSet MUST be signed with each algorithm present in the DNSKEY RRSet at the zone apex (see [RFC4035] 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

This document is a minor extension to RFC 4034 [RFC4034]. Also, we try to follow the documents RFC 3110 [RFC3110] and RFC 4509 [RFC4509] 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, Mark Andrews, Roy Arends, Rob Austein, Francis Dupont, Miek Gieben, Alfred Hoenes, Paul Hoffman, Peter Koch, Michael St. Johns, Scott Rose and Wouter Wijngaards.

9. References

9.1. Normative References

[FIPS.180-3.2008] National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-3, October 2008.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

[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.

9.2. Informative References

[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.

[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.

Author's Address

Jelte Jansen
NLnet Labs
Kruislaan 419
Amsterdam 1098VA
NL

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