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

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

Status of This Memo

This document specifies an Internet standards track protocol for the
Internet community, and requests discussion and suggestions for
improvements. Please refer to the current edition of the "Internet
Official Protocol Standards" (STD 1) for the standardization state
and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the
document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal
Provisions Relating to IETF Documents
(http://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the BSD License.
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. [RFC4033], [RFC4034], and [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 [RFC4034]. [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 8.

For interoperability, as in [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 10.

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 [RFC4034].
hash = SHA-XXX(data)

Here XXX is either 256 or 512, depending on the algorithm used, as specified in FIPS PUB 180-3; "data" is the wire format data of the resource record set that is signed, as specified in [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 of [RFC3447]), and EMSA-PKCS1-v1_5 encoding in PKCS #1 v2.1 (Section 9.2 of [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 8.

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 10.

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 to the hashing algorithm used in the signing process. Therefore, RRSIG resource records produced with RSA/SHA-256 or RSA/SHA-512 will have the same size as those produced with RSA/SHA-1, 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] defines new algorithm identifiers for existing signing algorithms, to indicate that zones signed with these algorithm identifiers can use NSEC3 as well as NSEC records to provide denial of existence. That mechanism was chosen to protect implementations predating RFC 5155 from encountering resource records about which they could not know. This document does not define such algorithm aliases.

A DNSSEC validator that implements RSA/SHA-2 MUST be able to validate negative answers in the form of both NSEC and NSEC3 with hash algorithm 1, as defined in [RFC5155]. An authoritative server that does not implement NSEC3 MAY still serve zones that use RSA/SHA-2 with NSEC denial of existence.
6. Examples

6.1. RSA/SHA-256 Key and Signature

Given a private key with the following values (in Base64):

Private-key-format: v1.2
Algorithm: 8 (RSASHA256)
Modulus: wVwaxrHF2CK64aYKRUIbLiH30KpFuPBje17E82ydQW1HYWHfoGm
          idzC2RnhwCC293hCzw+TFR2nqn8OVSY5t2Q==
PublicExponent: AQAB
PrivateExponent: UR44xX6zB3eaeyvTRzmskHADrPCmPWnr8dxsNwiDGHZrMKLN+i/
                 HAam+97HxIKVWNHD2ba9MF1SA8Cu9dcHZAQ==
Prime1: 4c8IVfUlAVXGW emitter 7fbzdC6U82fduE6KkSWk=
Prime2: 2z2pBE82XVnL74jqG4zIN1dfHjEGEtjJJ3RtaYDugvE=
Exponent1: G2xAPFfK0GxGANDVNxd1K1c9wOmmJ51mGbzdKFFNFMeK=
Exponent2: GYxP1Pa7CAwthMh8SAGX594q2VofOMhd6YFCNyeVpKE=
Coefficient: icQdNRj1ZGPmuJm2TIadubcO8x7V4y07aVhX464tx8Q=

The DNSKEY record for this key would be:

example.net. 3600 IN DNSKEY (256 3 8 AwEAAAcFcGsaaxdgiuuGmCkVI
 my4h99CqT7jwY3pexPGcnUFT2R36p6qW4btoneskZ4cAgv4ds8P
 kxUdp6pDlUmObdk= );{id = 9033 (zsk), size = 512b}

With this key, sign the following RRSet, consisting of 1 A record:

www.example.net. 3600 IN A 192.0.2.91

If the inception date is set at 00:00 hours on January 1st, 2000, and
the expiration date at 00:00 hours on January 1st, 2030, the
following signature should be created:

www.example.net. 3600 IN RRSIG (A 8 3 3600 20300101000000
                  20000101000000 9033 example.net. kROCoH6u710QGy9qpC9
                  1lsNncJcOKFLj7GhuO1bu4teYp5VE9RncrSh2Nz85mwlMgNEa
                  cFYK/1PtiVYP4bgw=);{id = 9033}
6.2. RSA/SHA-512 Key and Signature

Given a private key with the following values (in Base64):

Private-key-format: v1.2
Algorithm: 10 (RSASHA512)
Modulus: 0eg1M5b563zoq4k5ZEOnWmd2/BvpjzedJVdfIsDcmuhHE5SQ3pfQ7qmdaeM1c6Nf8DKGoUPGPXe06cP27/WRODtxXgSUytk00kJDk8KX8PfA0+yBWyw7Un2DycKyn000Uuk8HPVtZeM01pHt1AgVnc8VjXZ1NKdyit99waaE4s=
PublicExponent: AQAQ
PrivateExponent: rFS1IPbJllFFgFc33B5DD1cleg08e814fFfOdODb5p6V7shpKa6AZQX8YAw6V4FFPAKW41QdHk5iYOw5yvFDcUGzaa88qbjyrDPSJenkeZ1ISUMSSq7AMFZe0lkk6WSn6k3thUVrs1qDoOv3SEIAsrB043XgrKIVE=
Prime1: 8mbtsu9T19v7KSHdCeprILQXQLxz1SZunSTln/OjvXSUtvD7x n2ZJ+LhagjBjldgMbcq2UB000QVcK3TS9GiQ==
Prime2: 3a6gks74doJb7yL4j4adAif4fcp72rGt7G5NRVDDY/Mv4TERAKMaQTKN3okKE0A7+x+Rv2K84mtTQLD11Lecw==
Exponent1: v3D5A9uuCn5rgVR7wV8ba0/KspdsiLgsoA42Gx1lvgvs7gJM MvVTDu/Zg1p12npLnbb/S/Qd/MSwyN1xQ==
Exponent2: m+ez59dsDvYQk+gxjOLWEyKg5xWYBEYFGa3BLocMiF4oxkzOZ3J PZSWU/hiFjp5rIV7aPP0Vmx+hNjYMPIQ8Y5w==
Coefficient: Je5YyhUron/WdOxjNAxDubAp3i5X7U0ufhJcyIggqwY86IEOQ/Bk0Dw4SC9xns1mmdBXW2Izd8LwuuK8FQcQ==

The DNSKEY record for this key would be:

eample.net. 3600 IN DNSKEY (256 3 10 AwEAAIdHoNTOW+et86KuJOWRD plpndvwb6Y83nSVXXyLA3DLrORUKN6X06pnWnjJQujX/AhyqFD xj1l3On9u1/1k7cV6r1Mr2DtcQ5FC1/D7QNPSgVsMu1J2Q8g pMptzNF1pPB1bWXjdtA7QZB1Z3FY12ZTSncorffcGmhoOL );(id = 3740 (zsk), size = 1024b)

With this key, sign the following RRSet, consisting of 1 A record:

www.example.net. 3600 IN A 192.0.2.91

If the inception date is set at 00:00 hours on January 1st, 2000, and the expiration date at 00:00 hours on January 1st, 2030, the following signature should be created:

www.example.net. 3600 IN RRSIG (A 10 3 3600 20300101000000 2000010100000000 3740 example.net. tsb4wnjRUDnB1BuI+t6TMTX7hjVnG+eCrWqjyjvvhjzQLl0YRoOe0CbxrVDY0xDzuJRa eUwlep94PzEWzr0iGYgZBWm/zpq+9fOuaqYJRfDqfReKBzaweOL DiIn8iP9g9vMhpvup6OLvpxWx9s9a2X1b1fNg0fthPgxddLw =);(id = 3740)
7. IANA Considerations

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

<table>
<thead>
<tr>
<th>Zone</th>
<th>Trans.</th>
<th>Value</th>
<th>Description</th>
<th>Mnemonic</th>
<th>Signing</th>
<th>Sec.</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>8</td>
<td>RSA/SHA-256</td>
<td>RSASHA256</td>
<td>Y</td>
<td>*</td>
<td>RFC 5702</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10</td>
<td>RSA/SHA-512</td>
<td>RSASHA512</td>
<td>Y</td>
<td>*</td>
<td>RFC 5702</td>
</tr>
</tbody>
</table>

* There has been no determination of standardization of the use of this algorithm with Transaction Security.

8. Security Considerations

8.1. 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.

8.2. Signature Type Downgrade Attacks

Since each RRSet MUST be signed with each algorithm present in the DNSKEY RRSet at the zone apex (see Section 2.2 of [RFC4035]), 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.
9. Acknowledgments

This document is a minor extension to [RFC4034]. Also, we try to follow the documents [RFC3110] and [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, Scott Rose, Michael St. Johns, and Wouter Wijngaards.

10. References

10.1. Normative References

[FIPS.180-3.2008]


10.2. Informative References


Author’s Address

Jelte Jansen
NLnet Labs
Science Park 140
1098 XG Amsterdam
NL

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