Use of SHA-3 (Keccak) and RSASSA-PSS in DNSSEC
draft-muks-dnsop-dnssec-sha3-01

Abstract

This document specifies the use of SHA-3 (Keccak) hash functions in DNSSEC. It also specifies the use of the RSASSA-PSS signature scheme for RSA keys.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on October 10, 2017.

Copyright Notice

Copyright (c) 2017 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 Simplified BSD License.
# Table of Contents

1. Introduction ............................................. 3
   1.1. Implementations (Editor: to be removed before publication) ............................................. 4
2. DNSKEY Resource Records .................................. 4
   2.1. RSASSA-PSS/SHA-2 and RSASSA-PSS/SHA-3 signing keys ............................................. 5
   2.2. ECDSA/SHA-3 signing keys ............................................. 5
3. RRSIG Resource Records ................................... 5
   3.1. RSASSA-PSS/SHA-2 and RSASSA-PSS/SHA-3 signatures ............................................. 5
   3.2. ECDSA/SHA-3 signatures ............................................. 6
4. DS Resource Records ....................................... 6
   4.1. SHA3-256 digest type DS Resource Records ............................................. 6
   4.2. SHA3-384 digest type DS Resource Records ............................................. 7
5. Deployment Considerations .................................. 7
   5.1. Key Sizes ............................................. 7
   5.2. Signature Sizes ............................................. 7
   5.3. DS Digest Sizes ............................................. 7
6. Implementation Considerations ................................ 7
   6.1. Support for SHA-3 Signatures ............................................. 7
   6.2. Support for SHA-3 DS Digest Types ............................................. 7
   6.3. Support for NSEC3 Denial of Existence ............................................. 8
7. Examples .................................................. 8
   7.1. RSA/SHA2-256 (RSASSA-PSS) Key and Signature ............................................. 8
   7.2. RSA/SHA2-512 (RSASSA-PSS) Key and Signature ............................................. 10
   7.3. RSA/SHA3-256 (RSASSA-PSS) Key and Signature ............................................. 12
   7.4. RSA/SHA3-384 (RSASSA-PSS) Key and Signature ............................................. 14
   7.5. RSA/SHA3-512 (RSASSA-PSS) Key and Signature ............................................. 16
   7.6. ECDSA Curve P-256 with SHA3-256 Key and Signature ............................................. 18
   7.7. ECDSA Curve P-384 with SHA3-384 Key and Signature ............................................. 20
   7.8. SHA3-256 as DS Digest Type ............................................. 21
   7.9. SHA3-384 as DS Digest Type ............................................. 21
8. Security considerations ..................................... 22
   8.1. Considerations for RRSIG Resource Records ............................................. 22
   8.2. Signature Type Downgrade Attacks ............................................. 22
9. IANA considerations ........................................ 22
10. Acknowledgements .......................................... 23
11. References .............................................. 23
   11.1. Normative references ............................................. 23
   11.2. Informative references ............................................. 25

Appendix A. Change history (Editor: to be removed before publication) ............................................. 25
Authors’ Addresses ............................................. 25
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.

[RFC4033] described how to store DNSKEY and RRSIG resource records, and specified a list of cryptographic algorithms to use. It was updated by [RFC5702] to add the SHA-2 family of hash algorithms using the RSASSA-PKCS1-v1_5 signature scheme [RFC3447].

PKCS #1 v2.1 [RFC3447] introduced RSASSA-PSS which is a much better signature scheme than RSASSA-PKCS1-v1_5. The main advantage of RSASSA-PSS over RSASSA-PKCS1-v1_5 is that analysis can relate its security to that of the RSA problem (Section 8.1 of [RFC8017]), whereas the connection of RSASSA-PKCS1-v1_5 to the RSA problem has not been proved. With RSASSA-PSS, an attacker also does not know in advance what the encoded message EM will be due to the use of random salt that makes fault analysis attacks more difficult to mount. Although no attacks are known against RSASSA-PKCS1-v1_5, in the interest of increased robustness, RSASSA-PSS is REQUIRED in new applications (Section 8 of [RFC8017]).

SHA-3 is a family of hash functions based on the cryptographic primitive family Keccak. [FIPS.202.2015] states: "The four SHA-3 hash functions in this Standard supplement the hash functions that are specified in [FIPS.180-4.2015]: SHA-1 and the SHA-2 family. Together, both Standards provide resilience against future advances in hash function analysis, because they rely on fundamentally different design principles." Now that SHA-1’s security is known to be weakened and the SHA-2 hash algorithms are currently the last line of defence for use with RSA in DNSKEYs, and in DS records, it is sensible to introduce the SHA-3 hash function family to DNSSEC now to prepare for any eventuality. The SHA-3 hash function family uses a sponge construction algorithm that is different from the SHA-2 hash function family which uses a Merkle-Damgaard construction, so the possibility that an attack on SHA-2 will affect SHA-3 or vice versa is unlikely.

This document extends the list of DNSKEY algorithms with the RSASSA-PSS signature scheme [RFC8017] using the SHA-2 and SHA-3 family of hash functions. It also adds DNSKEY algorithms for ECDSA using the SHA-3 family of hash functions.

[RFC3658] first described the use of DS resource records. It was updated by [RFC4509] and [RFC6605] to add SHA-256 and SHA-384 digest...
types respectively. This document extends that list with the SHA-3 algorithms SHA3-256 and SHA3-384.

Familiarity with DNSSEC, RSA, ECDSA, and the SHA-2 [FIPS.180-4.2015] and SHA-3 [FIPS.202.2015] hash function families is assumed in this document.

To refer to SHA2-256 and SHA2-512, this document will use the name SHA-2. Similarly, to refer to SHA3-256, SHA3-384, and SHA3-512, this document will use the name SHA-3. This is done to improve readability. When a part of text is specific for a particular SHA-2 or SHA-3 hash function, their specific names are used. The same goes for RSA/SHA3-256 and RSA/SHA3-512 which will be grouped using the name RSA/SHA-2, and RSA/SHA3-256, RSA/SHA3-384, and RSA/SHA3-512, which will be grouped using the name RSA/SHA-3.

The SHA2-224, SHA2-384, and SHA3-224 algorithms are not used in RSA/SHA3-256 DNSKEYs and RRSIGs. The SHA3-512 algorithm is not used in ECDSA with SHA-3. The SHA3-224 and SHA3-512 algorithms are not used as DS digest types.

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].

1.1. Implementations (Editor: to be removed before publication)

An experimental BIND implementation of this draft can be found in the "sha3" branch in the git repository at: https://github.com/muks/bind9

There is also an experimental implementation based on the ldns library, which can be found in the "sha3_and_pss" branch in the git repository at https://github.com/tjeb/ldns.

These can be used to check for interoperability by other DNSSEC implementations.

2. DNSKEY Resource Records

The format of the DNSKEY RR can be found in [RFC4034]. [RFC3110] and [RFC5702] describe the use of RSASSA-PKCS1-v1_5 signature scheme with SHA-1 and SHA-2 hash functions for DNSSEC signatures respectively. [RFC6605] describes the use of ECDSA with SHA-2 in DNSSEC.
2.1. RSASSA-PSS/SHA-2 and RSASSA-PSS/SHA-3 signing keys

RSA public keys for use with RSASSA-PSS signature scheme using SHA-2 and SHA-3 hash functions are stored in DNSKEY resource records (RRs) with the algorithm numbers as specified in Section 9.

The key size of RSA/SHA2-256 and RSA/SHA3-256 keys MUST NOT be less than 1024 bits and MUST NOT be more than 4096 bits. This also satisfies a requirement of the RSASSA-PSS signature scheme that for a hash function that outputs a 256-bit value, the RSA modulus be at least 522 bits long.

The key size of RSA/SHA3-384 keys MUST NOT be less than 1024 bits and MUST NOT be more than 4096 bits. This also satisfies a requirement of the RSASSA-PSS signature scheme that for a hash function that outputs a 384-bit value, the RSA modulus be at least 778 bits long.

The key size of RSA/SHA2-512 and RSA/SHA3-512 keys MUST NOT be less than 1280 bits and MUST NOT be more than 4096 bits. This also satisfies a requirement of the RSASSA-PSS signature scheme that for a hash function that outputs a 512-bit value, the RSA modulus be at least 1034 bits long.

2.2. ECDSA/SHA-3 signing keys

P-256 and P-384 ECDSA public keys for use with SHA3-256 and SHA3-384 hash functions are stored in DNSKEY resource records (RRs) with the algorithm numbers as specified in Section 9.

The generation of P-256 and P-384 ECDSA keys follows the same method as for [RFC6605].

3. RRSIG Resource Records

3.1. RSASSA-PSS/SHA-2 and RSASSA-PSS/SHA-3 signatures

For signature calculation, this section uses the specifications of RSASSA-PSS in PKCS #1 v2.2 (Section 8.1 of [RFC8017]) incorporating EMSA-PSS encoding (Section 9.1 of [RFC8017]).

The values for the RRSIG RDATA fields that precede the signature data are specified in [RFC4034]. The value of the signature field in the RRSIG RDATA follows the RSASSA-PSS signature scheme and is calculated as described in Section 8.1.1 of [RFC8017]. The message M used in signature calculation is the argument to the sign() function as specified in Section 3.1.8.1 of [RFC4034].
Within EMSA-PSS-ENCODE, the hash function "Hash" used is one among SHA2-256, SHA2-512, SHA3-256, SHA3-384, and SHA3-512 for RSA/SHA2-256, RSA/SHA2-512, RSA/SHA3-256, RSA/SHA3-384, and RSA/SHA3-512 respectively.

The mask generation function is MGF1 (Section B.2.1. of [RFC8017]) and the hash function used within the mask generation function is also "Hash".

The length of salt in octets MUST be equal to the length of the output of the hash function "Hash" in octets. The value of salt SHOULD be random per signature computation. A random salt value enhances the security of the scheme by affording a "tighter" security proof. However, the randomness is not critical to security. See Section 8.1 of [RFC8017] for the tradeoffs in security due to a non-random salt.

These RSASSA-PSS signatures are stored in the DNS using RRSIG resource records (RRs) with algorithm number as specified in Section 9.

3.2. ECDSA/SHA-3 signatures

P-256 and P-384 ECDSA signatures using SHA3-256 and SHA3-384 hash functions are stored in the DNS using RRSIG resource records (RRs) with algorithm number as specified in Section 9.

The generation of P-256 and P-384 ECDSA/SHA-3 signatures follows the same method as for [RFC6605], except the collision-resistant hash function "H" (see Section 10.4 of [RFC6090]) for P-256 and P-384 ECDSA/SHA-3 signatures are SHA3-256 and SHA3-384 respectively.

4. DS Resource Records

The format of the DS RR can be found in [RFC4034]. [RFC3658], [RFC4509], and [RFC6605] describe the use of SHA-1, SHA-256, and SHA-384 for the DS digest type respectively.

4.1. SHA3-256 digest type DS Resource Records

The implementation of SHA3-256 in DS RRs follows the implementation of SHA-256 as specified in [RFC4509] except that the underlying algorithm is SHA3-256, the digest value is 32 bytes long, and the digest type code is specified in Section 9.
4.2. SHA3-384 digest type DS Resource Records

The implementation of SHA3-384 in DS RRs follows the implementation of SHA-256 as specified in [RFC4509] except that the underlying algorithm is SHA3-384, the digest value is 48 bytes long, and the digest type code is specified in Section 9.

5. Deployment Considerations

5.1. 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 [NIST800-57].

5.2. 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/SHA2-256, RSA/SHA2-512, RSA/SHA3-256, RSA/SHA3-384, or RSA/SHA3-512 will have the same size as those produced with RSA/SHA-1 and RSA/SHA-2 hash algorithms, if the keys have the same length.

5.3. DS Digest Sizes

DS RDATA with digest type SHA3-256 has the same size as DS RDATA with digest type SHA-256 (32 bytes). DS RDATA with digest type SHA3-384 has the same size as DS RDATA with digest type SHA-384 (48 bytes). Corresponding to these existing digest types, it should be possible to understand the impact of the size of DS RDATA when using the new SHA-3 digest types.

6. Implementation Considerations

6.1. Support for SHA-3 Signatures

DNSSEC-aware implementations SHOULD be able to support RRSIG and DNSKEY resource records created with the RSA/SHA-2, RSA/SHA-3, and ECDSA/SHA-3 algorithms defined in this document.

6.2. Support for SHA-3 DS Digest Types

DNSSEC-aware implementations SHOULD be able to support DS resource records created with the SHA3-256 and SHA3-384 algorithms defined in this document.
6.3. 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. This mechanism was chosen to permit implementations of NSEC3 to coexist with implementations of NSEC that predating [RFC5155] and that do not support NSEC3. This document does not define such algorithm aliases.

A DNSSEC validator that implements RSA/SHA-2 and/or RSA/SHA-3 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 nameserver that does not implement NSEC3 MAY still serve zones that use RSA/SHA-2 or RSA/SHA-3 with NSEC denial of existence.

7. Examples

7.1. RSASHA2-256 (RSASSA-PSS) Key and Signature

Given a 1024-bit private key with the following values (in Base64):

```
Private-key-format: v1.2
Algorithm: 247 (RSASHA2-256)
Modulus: 0xP+0iFPdhzUUmeYeZZZvddMG1lkpbvbcjSH/mLf/XksiFHq/legqzLQd5QajI3Tc7bIcRuuHPtib2nKm7k4R1SduNxzUyv5z/T9MDOqlQrUOsBveuC5Wf1b+36PLjWJNqnzFkZ9wuQIDF0uDZwGnebWZDJavq306j/XTA/iZtc=
PublicExponent: AQAB
PrivateExponent: uVnMoR7JFTG5rGb1+IbzZQYC+d0kyXhN+lpwtQyEHqPiXA57KT8vgkYL04WFTrlX3ju6hcBFw4Nn6+fdF6Os6zXGgexNh2PqDG+BSSO8P+dH7hNiuV2qSONgkKrJco0aX0q0sAyo7RzRHkAtUUFum//2qMQ7wGZRaVk3FPsFmQE=
Prime1: 8BHCdC21Zfw8cs4IUKSDqg6JZh6GkdHIHyRpgtPQ7pSx99QtIbU9+VoTcJHw09TId7MOm3fZ4nrALYQHFow7gQ==
Prime2: 4RW9O6uh52sNxjpYVqheZj+6Z2LvkIPsbgJQYsqhNLr/vf5apact+WXz5pWMlHOguiXu8qiZa86B1dxmHAkuVw==
Exponent1: t1p5D86RSxE5Ad4GT8E2pj1wB0StNtXoaJCg3UD1xCJhQo0U4zfP25BGZKWyL7fGXFWvhGInUWi7Oogp+bilAQ==
Exponent2: u5c+q2iT+ydBx6AA19hjNJyQYnIWbz9D4TuUe4GdcTEYy+Qc8EqxClZqPBcPnvnvTrUmvJ6/nxXxJ6gUgfE06Q==
Coefficient: m9t6RWOcmP1MLC8YiaxLvsJ1MLe+JTiu+Tzx7plz7bVd9cw0SCbD/X+VXBiDheu2ZyaZ8tuprEX7FdjiTU1Hdg==
```

The DNSKEY record for this key would be:

```
example.org. IN DNSKEY 256 3 247 AwEAAdMT/tIhT3Yc1FJnmHmWWb3XTBtZZKW723I0h/5i3/15LIhR6v5X oKsy0HeUGoyN03O2yHEbrhz7Ym9pypu5OEdUnbjcc1Mr+c/0/TAzqpUK 1DrAb3rguVn9W/t+jy41iTap8xZGfcLkCAxdLg2cBp3m1mQyWr6t9Oo/ 10wP4mbX
```

With this key, sign the following zone consisting of 4 RRs:

```
example.org. 3600 IN SOA invalid. hostmaster.example.org. (42 43200 900 1814400 7200)
example.org. 3600 IN NS invalid.
example.org. 3600 IN A 192.0.2.1
example.org. 3600 IN AAAA 2:2001:db8::1
```

Using RSASSA-PSS with salt filled entirely with 0 valued octets, 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 signed zone (with DNSKEY) should be created:

```
Jansen & Sivaraman      Expires October 10, 2017                [Page 8]
example.org. 3600 IN SOA invalid. hostmaster.example.org. ( 
42 ; serial 
3600  ; refresh (12 hours) 
900  ; retry (15 minutes) 
1814400  ; expire (3 weeks) 
7200  ; minimum (2 hours) ) 
3600 RRSIG SOA 247 2 3600 ( 
20300101000000 20000101000000 30005 example.org. C9c2AuyA6rB3XL08i3PgDtMZe2+shNy/B94+ f1fdxYz1OVmm?+byEVVxmAqw?nEn3MFUGpw?j E2lThin2pY24j4f4ep2z1kDxWFTfNkwxgA1 nFGez1hJBUUpfxpIZWOGwkJIWL+sB3mS3M Z1EJZ1okin372909f6tLcZDfLck= ) 
3600 NS invalid. 
3600 RRSIG NS 247 2 3600 ( 
20300101000000 20000101000000 30005 example.org. y/qVMuKsW5dqkB2LQmTj+RJ1UcE8/JpLw7/x yj1wh8qtUxJ3YkkfeDbx7Lah4+zmZ7ebib2Q gSedJ/EZERTwsB7njLio/hoMTUIXD/BBgb3 LyNHJ7v6ujZ06HJ2a14+qtYAXo2PHDV7i4I AtOJQR1+Lz5Q/6d6zJKUHiHft6E= ) 
3600 A 192.0.2.1 
3600 RRSIG A 247 2 3600 ( 
20300101000000 20000101000000 30005 example.org. SjVvbsH77EZfZnnNfPyeoFxkPe8yj7Jhb4Td mhFab1lpaqjY3gyOUyvB165KrvUBf5m/qMS NqBJF7t8TmmsMkVpal90GLYmvkQexxv4qI/X PKZ++nyNoa9HObcjUFgL0x3jLc5K+sRfnYWw ojQjh+l10Kb3h3q3wawGVmRgZZW= ) 
3600 AAAA 2:2001:db8::1 
3600 RRSIG AAAA 247 2 3600 ( 
20300101000000 20000101000000 30005 example.org. Tkleo5JjLCmzd+JzgG1Pfan4YNvrsL0Z8J RME2LionhQGGALScHy4Yb3RQQ7/SA+516 nBlwr1F23Kh5dkO9ApefRyxn1SZP61mdOcBu tdq6MrKwqgYWY7Lw7qO05JPAz7X7du 0F4qOBe/cBC9wK6grc/02kc0IPos= ) 
7200 NSEC example.org. A 3600 SOA AAAA RRSIG NSEC DNSKEY 
7200 RRSIG NSEC 247 2 7200 ( 
20300101000000 20000101000000 30005 example.org. CNggBNHd8AmjG3tVG34Mb6oMyx10XLU645d aDvA/LGZ5qBF80z5W56rYzpcbU51rZBBBAb nscR73oq89BaHEmzQcspVkoA8ao/xRakM11 N491RKB5vCVR2XnVkhHSb9JDVsK2T2d+cWzDN3 O/0Fqj9cV1NI/eT1w29FyEy2uo= ) 
3600 DNSKEY 256 3 247 ( 
AwEAkDMT/t1hT3Yc1FJnmmHmWw3XTBtZKZW7 

Jansen & Sivaraman Expires October 10, 2017 [Page 9]
7. RSA/SHA2-512 (RSASSA-PSS) Key and Signature

Given a 1280-bit private key with the following values (in Base64):

Private-key-format: v1.2
Algorithm: 248 (RSASHA2-512)
Modulus: v4LMvpU2sPxQHPOos4PFROf1U02gmzkOdeBjWiY1iEsyDgaGEJ/3x1D4oIVHI9pMVS47JoQvvhnnOnJv5/tslA5ivWsTp0i6rFzY3+F+zDUCA1AcD/rcECgfizC/VZSHvH3aThpjqiwCN6HtC9ofPNqxAikdwMeJP3oUSl3Pg/Y3S8pX2ykHNoq2+tROcypY4VUmbFqJa6SAxBT8EeWgTw==
PublicExponent: AQAB
PrivateExponent: uIbklwIZN4F2A992/rmJ23IRPNoAVXAtkcDKmjNUw2WI7mC0ztIEIgXP+oNQ36fYgv7PubYGdopo9TUMxJ7KqQIPe+nvfvEiBTBVO6r/zOveAJXvq3RuNJ0DCBnhvMhWMha7rRcqp3FixJ9J7cBEwRmJQn+KjrrOZJ9zCFJZ+CQZ5yTTFAdrkjDtpFrg8XUSuDqo85/RFtFUQiMHNzLZsQ==
Prime1: 8ji5lppCo7FCVENMf+a9u5EpXNwH8P+VFHaw99NAKqEV+pWBS24Op8yoRxt6f7mmRe4FTNyTfkkdSpMo5aN6oa1h/vFo14ifFTMU46Vm8ec=
Prime2: ymed+9gYJ/z4ulOPOBrJV6BSVIZgE1hxSkyR68h8fzGvc6iPCf7+JsM7XrIK3Z5dxFQ8WBg7YgbKn05mD1dqU3sJJpIstvKdhvUmaJyVYVk=
Exponent1: J/A+eZyZ3E+/9hDarkQniKPYxBzrmksqE6O2bkaA0AabjyPTm9JbzEMsg/z9581+ow0qBpBgKXR4xfEZzzNzZvEltVmsxc0bHe28RgThwoU=
Exponent2: jWsESRhdGGN57cXARXUBxIWxwHj628lprn39Xn5/7ebrLaZR+qv9K1wxOSKw0NN7tFceqnaT1xPliwoj2XDW5hoZqiFaNg23Ufpz+rwzomlE=
Coefficient: 2hX/dV/0jj0IUyAbx5N1I2kIsjf9FJmQHQjktr63YG0CMMBMRNUWF2Y4B3Z3RJHHdeBRvD4r3q7JlkhXvuOWn1EyLFx8ZGOZVboKIcePgUU=

The DNSKEY record for this key would be:
example.org. IN DNSKEY 256 3 248 AwEAAb+CzL6VNrD8UBzzqLODxUTn9VNNoJs5DnXgY1omNYhLMg4GhhCf ... AgNQHA/63BAoH4swv1WUh7x92k4aY6osAjeh7QvaHzzasQIpHcDHiT96 FEpdz4P2N0vKV9spBzaKtvrUTnMqWOFVJmxaiWukgMQU/BHloE8=

With this key, sign the following zone consisting of 4 RRs:

example.org. 3600 IN SOA invalid. hostmaster.example.org. (43 43200 900 1814400 7200)
example.org. 3600 IN NS invalid.
example.org. 3600 IN A 192.0.2.1
example.org. 3600 IN AAAA 2:2001:db8::1

Using RSASSA-PSS salt filled entirely with 0 valued octets, 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
signed zone (with DNSKEY) should be created:
example.org.            3600    IN SOA  invalid. hostmaster.example.org. (43         ; serial
                      43200      ; refresh (12 hours)
                      900        ; retry (15 minutes)
                      1814400     ; expire (5 years)
                      7200       ; default TTL)
                      Jansen & Sivaraman      Expires October 10, 2017               
                      example.org.            3600    IN SOA  invalid. hostmaster.example.org. (43         ; serial
                      43200      ; refresh (12 hours)
                      900        ; retry (15 minutes)
                      1814400     ; expire (5 years)
                      7200       ; default TTL)
                      Jansen & Sivaraman      Expires October 10, 2017               
                      example.org.
1814400 ; expire (3 weeks)
7200 ; minimum (2 hours)
)

3600   RRSIG  SOA 248 2 3600 (20300101000000 20000101000000 50019 example.org. L1qNhZM2thJKDab5lkkfrzn9TtIMyWSZ+7+yOZU Uk9g9j6aCzezPNiPer9A0FtgDaxFU21CRDox kGeWjhqEN1JGOxA7robPGj0TLWAAYbzsihBE ehqkpDTJHsmTv3lnjiA0FaalFKwisCRI1HG9 t7T9sZMEc1G25a4izULX6PiKAjbBeggJ6sGK 6OgCbufE3yTwJTPb3/WS1fPv/bRntETWA-- )

3600   NS   invalid.

3600   RRSIG  NS 248 2 3600 (20300101000000 20000101000000 50019 example.org. Sj3jxLM0kK0UdOY9O9Zhrup+0iafH8yKD2I a2m1S8jnJrWwQplg/RRCoM+9B5rrs9A0N2Jq? ihWewm59Jk5ubmQP/zct/5UrfdIPNpGbG? epJ5aMVvفو500QeqL/yChwkkZcpVd9yzzYqV+ Sx6mhMj9SSqS/CBZZzjwJopOP4zahha41Ry J/3PG3oOhQ?hAigUcNgO4AwxAoVd/3yQQ-- )

3600   A   192.0.2.1

3600   RRSIG  A 248 2 3600 (20300101000000 20000101000000 50019 example.org. G2Y8uKkZ2pRhtL9Dh6NRq8GES4W0h9A0FtcNc PHvVXAnuMdh8lwgmXeT?66HuhFw8Ghj0WJ XkpG8k1nCphsP51eSF0ger6vlISliyCwx/2Khw5 4cUufvkbZ3e3lyHOS3XwLDICT6S755vaxv CjnFaf14AznPOS5+55nq2Euuq?stve88mU0Q Wq4FZOn0NlIY1dBRfzpCKBSs0Ww5BqtPQ-- )

3600   AAAA  2:0001:d8B1

3600   RRSIG  AAAA 248 2 3600 (20300101000000 20000101000000 50019 example.org. MY2ha2+UIdheHSEeBLqlb6s9gTC07yUQkz3c yM3A3A1s78y/nz9GsEUjP6jGmMtc0Qa64mx WF1150o/Lwrum/HLwvoXc1wZcUeC57ipwQY z1qUNNbc1KILChzmqO7x1caK/kj88RoSpz rGWNbL0nL251OLy30dcvznjwzmn2LaA1 g805ps4+p5QbeToASNGGPR84LpR7j4nwrw-- )

3600   NSEC  example.org. A NS SOA AAAA RRSIG NSEC DNSKEY

7200   NSEC  NSEC 248 2 7200 (20300101000000 20000101000000 50019 example.org. l2RkbZqiyfMWNVlvt/FZII7Q/DVSsCqVE JsiE+bjbboyloilHdnia92Wt/apob6MVHgAg KX3EII+WOGuPBH3P2x2vFWgh1EU30cTwv JCS1cQ98pBzliTwMVAPcP0lMUFJ2ZMzLZC9 Jyv5FW2UcLUK64BC5saj0QWPFpWkWjM19jld weyYT+oCKY/GurJbRe6Jo4r3Mgsq1Pdca-- )

3600   DNSKEY  256 3 248 {
5.3. RSA/SHA3-256 (RSASSA-PSS) Key and Signature

Given a 1024-bit private key with the following values (in Base64):

Private-key-format: v1.2
Algorithm: 249 (RSASHA3-256)
Modulus: uI99tnWEAZ5j8hnh29acjTWKUncLZpGWYCWjmz7KB7q8NCiGdA7dgkIBpGrsry0jF8PVGP8jm2omdMaPDX2N0UcEVKrUSKczNQb3Kdiihl1J8/IC9KZuHqQJHr8E4Gu/S4P1EbpaM00F1YPCkldl7yTyXEA6waP2Qs6lfRETffU=
PublicExponent: AQAB
PrivateExponent: ceGgqZBzxufsNfxAgH05lmx+EIqCT2TwTB2NiYLB+OkBrpF+/WgayIBgMQsFRsZsTAK7oDP2zbQ/THkk1ict9PHByDAAedOo+sjYqja7/NMqHZV2y5nfOV2gr/Qkx8Ns/JhcZ6bD0TtS+mTTGZPKxHZYoZKp/EYaRpY/FH/tgBU=
Prime1: 8a4Tyux12glzCP4cLndnDi2MT9M4WRR0B+8SjU1zoZVgOiF7WnCD6go3LAGl8SbiMzX491cJFKuK7/0qY4wTcw==
Prime2: w37/PBybwbTCtWJeGQo5sZUmAfcB4G9KPb0Xx7attTlVcvS3BsNxQ6u5CJS6PkxrRLJhObY0co97esbRlfXe9w==
Exponent1: X5pyH/LcR+03AVasRUFclgI0oBs5DhwGLmFHYHhEBqZ1k2lNR6B8vmdeHd1lDHlKP+HY49cdM30MkBUA4LI3uw==
Exponent2: P7FYptULSgkChuYNkkrqkRju0SUQz3Zy0bqRzNePsMOFO3bPSrzSYiHInysVosZzDGaxloPugoSMzmuITTtV8Q==
Coefficient: NdPPfYznkez2NNKsVydeZleq+jOBaQ3O98YZteXreOrH8L+pqKxkymKIvqjiTzWdA+fDV7KfFrbv0ZFwGymsNQ==

The DNSKEY record for this key would be:

example.org. IN DNSKEY 256 3 249 AwEAAbiPfbZ1hAGeY/IZ4dvWnI01ilJ3C2aRlmAlo5s+yge6vDQohnQO 3YJCAaRq7K8tIxfD1Rj/I5tqJnTGjw19jdFHBFSq1EinMzUG9ynYooZd SfPyAvSmbh6kCR6/BOBrv0uD9RG6WjNNBdWDwpJXZe8k8lxAOsGj9kLO pX0RE331

With this key, sign the following zone consisting of 4 RRs:

example.org. 3600 IN SOA invalid. hostmaster.example.org. (44 43200 900 1814400 7200)
example.org. 3600 IN NS invalid.
example.org. 3600 IN A 192.0.2.1
example.org. 3600 IN AAAA 2:2001:db8::1

Using RSASSA-PSS with 5 unused octets. 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 signed zone (with DNSKEY) would be readable:

example.org. IN DNSKEY 256 3 249 AwEAAbiPfbZ1hAGeY/IZ4dvWnI01ilJ3C2aRlmAlo5s+yge6vDQohnQO 3YJCAaRq7K8tIxfD1Rj/I5tqJnTGjw19jdFHBFSq1EinMzUG9ynYooZd SfPyAvSmbh6kCR6/BOBrv0uD9RG6WjNNBdWDwpJXZe8k8lxAOsGj9kLO pX0RE331

The DNSKEY record for this key would be:

example.org. IN DNSKEY 256 3 249 AwEAAbiPfbZ1hAGeY/IZ4dvWnI01ilJ3C2aRlmAlo5s+yge6vDQohnQO 3YJCAaRq7K8tIxfD1Rj/I5tqJnTGjw19jdFHBFSq1EinMzUG9ynYooZd SfPyAvSmbh6kCR6/BOBrv0uD9RG6WjNNBdWDwpJXZe8k8lxAOsGj9kLO pX0RE331
example.org.  3600 IN SOA invalid. hostmaster.example.org. (  
                   44 ; serial  
43200 ; refresh (12 hours)  
         900 ; retry (15 minutes)  
1814400 ; expire (3 weeks)  
           7200 ; minimum (2 hours)  
 )  
3600 RRSIG SOA 249 2 3600 (  
20300101000000 20000101000000 23809 example.org.  
Uwq407WnX3WgD4gqrE931DqCByyWqf6+YfZe  
vRCTzMe+/q/36pWhYhej6wI3Fo2JReMeL85  
IEdQNEUocZ4SyfbnC/x44Tj3xF1im40dWy  
/HDLadAlcFL8ZVxd6KNPBoGsZmWqdePguC  
Kvv6KpZ6smQhlPf1NhmcvUajG80= )  
3600 NS invalid.  
3600 RRSIG NS 249 2 3600 (  
20300101000000 20000101000000 23809 example.org.  
WXtpjYg92GDybn01HbzwHij8pccxIcalit6e  
c1k1YFER1/Gw3oroFvHei7728WuyGyjm7QnXP  
/aevYGX7tAmObgKRhh089k2tDj8Ku6aKYRvnVh  
jobJi2WesKBMCCswchjK64WJVW90PwWI7/j6  
D8fwTySTSmpQXn7mG/0ynIiwruw= )  
3600 A 192.0.2.1  
3600 RRSIG A 249 2 3600 (  
20300101000000 20000101000000 23809 example.org.  
K718GCTXBALK3gljrySt4PvHrPFwUYCN  
v97mU25mhBerDLNlyNTSCeMQFwDNyXvy7VBR0  
8dpmnmZ9GiHd4oaj4SCkCz7QkNInqF77sZe  
2jryHl8Vu7T9JqFaijJ3yUHLvngGabc40qBC  
zTtP8g1I3COpnnp6Q0kLxyjWVh= )  
3600 AAAA 2:2001:db8::1  
3600 RRSIG AAAA 249 2 3600 (  
20300101000000 20000101000000 23809 example.org.  
e8EgXwko7vVvU832W8qEIs+51HUfgkowoichs  
9L7U5eX1axryn7c3c7WvFy1hNGLxrZGU7e  
rVR+0QG989x1lwFSHeETryq/55UAp0OeoAFyJ  
3D+2ZXiOgG3HWP+zZ2R3tQxOB1lNHFPXw  
14J0wPdp.fBj4jczG6Ywd5VAd3M= )  
7200 NSEC example.org. A  
7200 RRSIG NSEC 249 2 7200 (  
20300101000000 20000101000000 23809 example.org.  
rfCOWKbnLoXuLPqE5fhq?yN10ZB2e0cCj7  
8c4DRDMIXistBFroNhYmgTTratXojbJGOC4F  
nbA3k5Oh91ReSevASHFD95vAy5KuWJYwMx  
hLROhu9TJE7i3VgYt6rEHQIMr0Orzy3dao48  
12mcdW14MgoDyJAxtBdOGZytEFY= )  
3600 DNSKEY 256 3 249 (  
AwEAAbiPfbz1hAgEy/I24dvWn101JL3C2aR  

Jansen & Sivaraman Expires October 10, 2017 [Page 13]
7.4. RSASHA3-256 (RSASSA-PSS) Key and Signature

Given a 1024-bit private key with the following values (in Base64):

Private-key-format: v1.2
Algorithm: 250 (RSASHA3-384)
Modulus: xHuxiHax4XcfW9yCIdCVdrqs+L1lfTZKdOK7C+J8yDptcyS7DC8Su0X4hqJxA3M0gZFfpwSpuc1/XSwm0pDCqByy1qehIZgJMQ9dm6whqokGgqcpOxEbLhKDHoUl6dq6MVZAoys2wYgpEwK9E0GPx1OT80EeO/8txqyIx1b3X1s=
PublicExponent: AQAB
PrivateExponent: vFr/xBxVRhkWPM/VCGmW/uzR6NpXsoMbOZYpTalfietJBTrO/U0bHeBj8V1EDdShHxynn8r+khoH4N/0j6MqlqEnKmL7lTDeGV5ezKLu3uLFa6RISolasqpQBqptImJ+hbXtozDKPhfjI/+d9FZBB6J1g2RlwujGX6VJMbSefvE=
Prime1: /fmeKF6OHGM9aWJq4j2/tNgbdTdy9tP2pi7VG4w7MZcXtt5jRuwDt9RfBb0i01+KOROWyIklTeHC3OIdU6otLw==
Prime2: xgy6/HX5aChVos1eunk1ZezvweGNfBuZr4TcpcTShzLs8ftGs/fAZ6Ea44p7EZizB1yaEspfcvTMHFnC709dlQ==
Exponent1: 3UV/P9ixo5XqyUgPqzD1NxAZTBSVOusNN1gSH0AbymbDKHW0tPOngZ+rcgqIrvPML1IbyneCYspQxbTSrDPVzQ==
Exponent2: BOFlbjk+ByoPSi7Dadb40OUw11dGlEtd0yxz/4XFJl3D5wapLGArlqIqtnbAJ6ParZDDnzjrdzq/GOfBXQJYrQ==
Coefficient: NPxHl0td8V/7Sk7dnGfF6Fbde3Kwt8PUUsVulh3rsr1wjmWeW6JFBxd8R104k+HicCXrLj+YthGmLS3jCwnidQ==

The DNSKEY record for this key would be:

example.org. IN DNSKEY 256 3 250 AwEAAcR7sYh2seF3H1vcgiHQlXa6rPi9ZX02SnTiuwvifMg6bXMkuwwv ErtF+IaicQNzNIGRX6cEqbnNf10sJtKQwqgcstanoSGYCTEPXZusIaqJ BoKnKTsRGy4Sgx6FJenaujFWQKMrNsGIKRMCvRNBj8dTk/NBHjv/Lcas iMdW919b

With this key, sign the following zone consisting of 4 RRs:

type  example.org. 3600 IN SOA invalid. hostmaster.example.org. (45 43200 900 1814400 7200)
type  example.org. 3600 IN NS invalid.
type  example.org. 3600 IN A 192.0.2.1
type  example.org. 3600 IN AAAA 2:2001:db8::1

Using RSASHA3-PSS with filled entropy, 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 signed zone (with DNSKEY) should be created:

example.org. 3600 IN SOA invalid. hostmaster.example.org. (45 43200 900 1814400 7200)
type  example.org. 3600 IN NS invalid.
type  example.org. 3600 IN A 192.0.2.1

type  example.org. 3600 IN AAAA 2:2001:db8::1

Jansen & Sivaraman  Expires October 10, 2017 [Page 14]
Internet-Draft
Use of SHA-3 (Keccak) and RSASSA-PSS in DNSSEC
April 2017

1814400 ; expire (3 weeks)
7200 ; minimum (2 hours)
}

3600 RRSIG SOA 250 2 3600 (20300101000000 20000101000000 54407 example.org.
17x4t2CwGks6qLxRxbdp+pafk277rz91vug
UFyU+TmOzPYqQo2MojJn8TVuje9vV4EnuzZ
cTZck044r9Xiqathh4tYsaJfK8otr30DYWYd
GOV719RbypfJOk9FW4+rcgsSFTu323+a78
PuGhs5or7UYGll/d0///WraW+Zg=E- )

3600 NS invalid.

3600 RRSIG NS 250 2 3600 (20300101000000 20000101000000 54407 example.org.
clo2/g51y3eo3E3+28Ot1k4vg4sE8MEIHdel
rD35/XAOoz2QFH0mBzEYGTk7Dxv8tA0yj
M9xtoP9H1lxmDF19yjKsTTNpXmbcbxA/NNH
khoqX3EszLZZD1t7brDqKt+jCaalkxMe6JNH
m03CrTj6b2Y4TROa8swzElwMSC= )

3600 A 192.0.2.1

3600 RRSIG A 250 2 3600 (20300101000000 20000101000000 54407 example.org.
UXoGfLBw5u4b0bMrUvF6C4Yn/WspMpV5ARf
Z2aZPBABB52TdmLx0p4R4XG902NlQbKCVs
4qLi2MutsvD8ABN3IjCvNefty817+wdUnK
HFLk80+/+GCBO934m1JTKnazGPhUJt1ZucZV
j5N1o+OVLQfCgKtUjg+Y63J5V0= )

3600 AAAA 2:2001:db8::1

3600 RRSIG AAAA 250 2 3600 (20300101000000 20000101000000 54407 example.org.
hMN/J/z5EyMcCh9Rg3povhidhSRQCQeITWyhX
i7+prwrtJ0CccOmakacjeQJuKBOEkeX0zzUpLL
nXY3uobZCvWh3ouHxZ+y9CgLuegRjfk2Sr
KrBML1zXceqg2zjxr7UJYn9ty6sJe0jQbLk
LDE0W7fPPSLPELa0S8kS6Z5X/6E= )

7200 NSEC example.org. A NS SOA AAAA RRSIG NSEC DNSKEY

7200 RRSIG NSEC 250 2 7200 (20300101000000 20000101000000 54407 example.org.
ZTSVW0Y5H0HY6OKhBrJaqDhDpJgXz6i6hA5/
Nuti0JgtXr+55PGdp1IffS3Q4vuqgbw0jD1
EcSGuGpV9lN4qW2YwSAL3e5Kw16RwbKz
G5YfWfduyzPZ57nGdykzeNOZBRb1bEpLUEzEP
/u+TQCtRLDSTMv4s6ig9N9d2g10= )

3600 DNSKEY 256 3 250 {AweAAcR7sYh2seF3hi3vcgiiH1Qx6aR12X02
SnTlUwifM5gbXMkxwErtF+IalcQnNIGGR
X6cEgbnNF10sJtKQwqgcstanoSGYCTEFPZus
IaqJBoKn1TSRgy4SgX6jFenajufWQKMr3sG1
KRMCVRNB18dTk/0BHev/Lcasi1MxW919b

Jansen & Sivaraman Expires October 10, 2017 [Page 15]
RSASHA3-512 (RSASSA-PSS) Key and Signature

Given a 1280-bit private key with the following values (in Base64):

- Private-key-format: v1.2
- Algorithm: 251 (RSASHA3-512)
- Modulus: o+YkFXrbuWtwzgjWTMxKWL/mxKmZiIEwZQocnh0XN8ON6AIFc+aECjkxwO5pWG171NCXt2acYWnKakpCmpiSHh9ggj8hL5O67Zs409xo0vqRpXzxY27IvBtKNurtD48RiPknLh3fEhuRnHEj8X2fpuOUx0yN5wOZx3PRjNxMeLnTglxHfRqah/tApQnCTvBAWX5vSYmPP1u/4I/UR1Zpyw==
- PublicExponent: AQAB
- PrivateExponent: TJqZTOzSW7SK0dGxj82ABkETM+HtH676Fo+GVqRUIL0my0R+lfAs0LZwubL0y97IHOytrIuqFaGjeNBilu0uhiO2MMoe0aTjnoCJLAR9ffXdqZb1FGMn8kWkmmtZJbm3LzFYHMs4B0exGq4vI2DfX5UF0LZV1YN4WIk2jgMPgRdJRZOOr0ZyJs8dz4VwhuVZx6SRa4ADB22QIRUdCCEESQ==
- Prime1: 0fpRrO03qcRgQpwNiiw0sjBguAClUVMY9H+ZLwUrAsiP65/ikHOOXTve7aAW/OMnAmKdmpaA0jeMiYdwidMcdwVJbZM0qHsqkxrVZmtgFy8=
- Prime2: x9Jgn/DLIVzcPl8VazyWcn51hbM2xd8J5fZYp/ZPVJBDlfvlICT6YbpYg8CyPjUpoDM4JnAH9v0sICO7GgrvQIY5XEYnLmUttdBj8+D58CU=
- Exponent1: lXLZcQABrzYS4TXauS5Pb0fZfv0OrPw89cBfkcTW4QtIzAanJfLpL9iuCWj5E5LFMABqdh2KoJRi1XvtkFsOlnPP2Ep+ny/SlJLzsgrYgIc=
- Exponent2: fsVfe9keZhotuHxGcHRN1nGYSax7MWnhM73oXRcNGU81MbBPmuca2mmIwn28F29O603Tb79frjjMh89jYpBRXZRKS9pN/Uc/iruczhqLNuk=
- Coefficient: JF5wby8oSnh2Hqff02l7tA80wNf99YWUPSn3yHfuoQKgn274V2N/QE4XgcpJd+ioSkKNX+GV6RpG+b8gUiR1hCxHBPpmeb/QcA9ivnrW0L0=

The DNSKEY record for this key would be:

```
example.org. IN DNSKEY 256 3 251 AwEAAaPmJBV627lrcM4I1kzMSli/5sSpmYiBMGUKHJ4dFzfDjegCBXPm ... kaV88WNuyLwbSjbq7Q+PEYj5Jy4d3xIbkZxxI/F9n6bjlMdMjecDmcdz 0YzcTHi504JcR30amof7QKUJwk7wQFl+b0mJjz9bv+CP1EdWacs=
```

With this key, sign the following zone consisting of 4 RRs:

```
example.org. 3600 IN SOA invalid. hostmaster.example.org. (46 43200 900 1814400 7200)
example.org. 3600 IN NS invalid.
example.org. 3600 IN A 192.0.2.1
example.org. 3600 IN AAAA 2:2001:db8::1
```

Using RSASSA-PSS salt filled entirely with 0 valued octets, 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
signed zone (with DNSKEY) should be created:

```
example.org.            3600    IN SOA  invalid. hostmaster.example.org. (46         ; serial
3600    RRSIG  SOA 251 2 3600 ( Jansen & Sivaraman      Expires October 10, 2017               
```
20300101000000 20000101000000 23118 example.org.
OLszlePpxC9kXYEHP+xnQ/5VVGUuIECXHzEG
ksSPKtAmztjP3GyZxNQsahV7yKkkd6TX
h4S9pho8ZW9dsbPdcjZc1w15aL+GvzUXHsEGJ
chObfuAIAPw3I03V5/8KUH6o1CCTDyBleP
sa1/HH+Gk6mblU1vN6BCKjT8U2wY2TItmCry
a9heSY0U8OroQplzlJhtmyU46Ltfd7tg==

3600 NS
3600 RRSIG NS 251 2 3600 (20300101000000 20000101000000 23118 example.org.
LtjteIlhqrJWOJDvVHB2YDpPc62N40uGe
GoSjS9pfU8Ete8K4T+TQGeF9s5QPMKMI+
LtdSY4GpTLBSvZpUw1ht4hZw5mKURWDJ7p
+2R14ie45hS91R79048ZCxe7DbqA+3JWhbLVvo
KFamsFw1StpW5G700+i33Y0TR12S/7TF
p3ewL2w0yrMaSzzqj+UM3oLXMyYoD71A==
)

3600 A
3600 RRSIG A 251 2 3600 (20300101000000 20000101000000 23118 example.org.
HcofonaxmSgcmorCkr6f0mm3K/6zbbQqYse5
u/dmqN04JGj080fimRXwWe2uaUQCTSITYD+
BONJa9botX36udJgtn+Uygz+xFSrF/W0lb9X
GrKBzRUXWKL8s/gCjJMN1vChsWcF1h4+w4K
QAxWmpm2nNdbL83D1Ep+p+RqLgsawubhwc2t0
UM6Kljgsx8sYEDDDVke6f0URKFWB0bsey5pQp==
)

3600 AAAA
3600 RRSIG AAAA 251 2 3600 (20300101000000 20000101000000 23118 example.org.
AvBYm06oMCAOQIlsDps05+cRUX+vZQvqahN8
JnT68vb1y1xU0a5BlxQv7Irjjm7af73Ny
6tdZfu0Qou0SpfCsa22cPC45r5PZvWZejGc
Fcf61ONEMftv4d3ag6CIn9W7j74gEAgmnp+j
uB7/hYK12A2/shgDr0S1OEax2YehBNXvDlvH
aSwQoLrW25zN4EgnVXMRQK20I0HyKrR==
)

7200 NSEC
7200 RRSIG NSEC 251 2 7200 (20300101000000 20000101000000 23118 example.org.
MeDqWU8KujjIl5ZLBef0qgvyuQ6Nim+IPDFMA
j2UKov41KpQt2r9yiY+71L8ow/PRVvb0Mm
VfVUTIKCWB1bfAh0F2BFAJTIaEFElnUsTaa
jocNDrsEn8VoEH882r2wjgD05hmm52v7ZCT
QqrRgrz2BUCHu9dDHNfauiE0mrcnCqluFRJR
DafCZezyz3pZV1dyFDw2L2RzkyKduHug=
)

3600 DNSKEY
256 3 251 (20300101000000 20000101000000 23118 example.org.
AwEAaApjMjB6271ucM411kzMSli/5sSpnYIB
MGUKhj4dPzfDjegCBXPeboAs05McDuavHve9TQ
17dmmGFpynmpQQqyKh4Yf11/1S+Tuu2bGOnPc
aNL6veV88WNuylWb5Jbq7Q+PEYJ5y34d3Xib

Jansen & Sivaraman Expires October 10, 2017 [Page 17]
k3axl/Y9m8y3lMOBM7wOBvodzjYaCThi504zc
R3JansmFm/QM7w8c5rWQy4b50Mjy9kbC51EGc

3600 RRSIG DNSKEY 251 2 3600 (20000101000000
20000101000000 23118 example.org.
3600 RRSIG DNSKEY 251 2 3600 (20000101000000
20000101000000 23118 example.org.

7.6. ECDSA Curve P-256 with SHA3-256 Key and Signature

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

Private-key-format: v1.2
Algorithm: 245 (ECDSAP256SHA3-256)
PrivateKey: FHj8A/R6a/L9gP0cEyi/2ILg8d70maxr3332F2noED2c=

The DNSKEY record for this key would be:

example.org. IN DNSKEY 256 3 245 5DuYfUIL3CQAibLVRZkHNX8RsmMgXYMVw5hU6UhsF0NV4wT Ve6eFMTzJMMZ21Uk+611YxSL5a77g==

With this key, sign the following zone consisting of 4 RRs:

example.org. 3600 IN SOA invalid. hostmaster.example.org. (40 43200 900 1814400 7200)
example.org. 3600 IN NS invalid.
example.org. 3600 IN A 192.0.2.1
example.org. 3600 IN AAAA 2:2001:db8::1

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 signed zone (with DNSKEY) should be created:
example.org. 3600 IN SOA invalid. hostmaster.example.org. ( 40 ; serial 43200 ; refresh (12 hours) 900 ; retry (15 minutes) 1814400 ; expire (3 weeks) 7200 ; minimum (2 hours) )

3600 RRSIG SOA 245 2 3600 ( 20300101000000 20000101000000 43839 example.org. LWigv/bGi1b3Oy8VwxioCNv9Gzcmkm3l90x dRR2EE8m?mAB6STRkCAWb/W6FS01dCQP15gL 8cCbo8yepcmhtFw== )

3600 NS invalid.

3600 RRSIG NS 245 2 3600 ( 20300101000000 20000101000000 43839 example.org. I/z715Q7I6GeC/NynbXGg5qtbVh9DBMFuvX2 6eO600eOeRC7As6/oQmb1kXaHPpLj4amg+f/n HnJHUFyWeLuq+Q== )

3600 A 192.0.2.1

3600 RRSIG A 245 2 3600 ( 20300101000000 20000101000000 43839 example.org. PuehYlyx2USSTellmmCmu0fe9Lty4IMB7BMY q106Q95EmD9NE93aNh/W3jy3aX5rrZ0munm UDLxTS/b3WTI7A== )

3600 AAAA 2:2001:db8::1

3600 RRSIG AAAA 245 2 3600 ( 20300101000000 20000101000000 43839 example.org. jmqWqjCvCC1JLGpOTUYqBp4w3x3RQ4U1Qaj Wg1w/PZUX2L931+UScQCgxEeUMEsPBQiDRD2 ngjAaSy3EPacAmg== )

7200 NSEC example.org. A NS SOA AAAA RRSIG NSEC DNSKEY

7200 RRSIG NSEC 2 7200 ( 20300101000000 20000101000000 43839 example.org. 7TtbaBCoVLjTGx3yDVDoCGsG3+1Fd4C4S9z1 jSOP1YfR3Kn1BPE+9fy1/5Yl99JDLv+AIJl 49gk+PBru63EAA== )

3600 DNSKEY 256 3 245 ( 5DuYFUI3L3QA1bLV2RkHNX8BsmMgXYMwSwS Wv5FqhULW6uhFONV4wTv6eFTWrJMH421UK +SI1YFwXSL5a77g== ) ; ZSK; alg = ECDSAP256SHA3-256 ; key id = 43839

3600 RRSIG DNSKEY 245 2 3600 ( 20300101000000 20000101000000 43839 example.org. oRrJQrqVwC+FAtxUQEl1LoPUXZEcOILkG1P kYoOt5/K9/PLTIPbU9szJeVjWslL8FBHetsq NWWy6KBPbRZQGw== )
Given a private key with the following values (in Base64):

Private-key-format: v1.2
Algorithm: 246 (ECDSAP384SHA3-384)
PrivateKey: FaHBWT7qWcJF2J4ExUPgBZ1poxJ/Cwvzv6+BF5rGT3KuIs83ABt51ITt4hVwaGfc

The DNSKEY record for this key would be:

example.org. IN DNSKEY 256 3 246 KQdbXXFXMQBV7lAOrRwFYRitDHNxZEXbVYz7FxAkwlGNYdkEePKE7Wfz Apttla0sMW0E+1sJAm8Cf-yuoqSnXpvo6YdZ2q7Jof2z98rJF11Ma 9uS0F97TS64cOY

With this key, sign the following zone consisting of 4 RRs:

example.org. 3600 IN SOA invalid. hostmaster.example.org. (41 43200 900 1814400 7200)
example.org. 3600 IN NS invalid.
example.org. 3600 IN A 192.0.2.1
example.org. 3600 IN AAAA 2:2001:db8::1

If the inception date is set at 03:08 hours on January 1st, 2000, and the expiration date at 00:00 hours on January 1st, 2030, the following signed zone (with DNSKEY) should be created:

example.org. 3600 IN SOA invalid. hostmaster.example.org. (41 43200 900 1814400 7200)
example.org. 3600 IN NS invalid.
example.org. 3600 IN A 192.0.2.1
example.org. 3600 IN AAAA 2:2001:db8::1

James S. Silverman Expires October 10, 2017 [Page 20]
7.8. SHA3-256 as DS Digest Type
Given a 1024-bit RSA/SHA-256 DNSKEY with the following contents:

```
example.org. IN DNSKEY 256 3 8 5AwEAAbljrZZb1Qyq8ui+vnYL5exWSrQYFkCFD6VvJoJr5ADo7CxZiyxusJM6oVHF7pA22rKJqjgIR9lksZ1+nT2WcwdXQuAFLrLFAI5L42mQKOHSx1S3vHosO0iSIX47IyyR2O+J9qLhy7B+T4cJzAq2dOtSziqL1l5BCtw5ZNYJX8N
```

The DS record for this key with digest type SHA3-256 would be:

```
example.org. IN DS 25803 8 253 AE03EA9388D4BA12725999B8E2C4ED14E06EAE8B78229B81154F61FE8EDBAA5F
```

7.9. SHA3-384 as DS Digest Type
Given a 1024-bit RSA/SHA-256 DNSKEY with the following contents:

```
example.org. IN DNSKEY 256 3 8 5AwEAAbljrZZb1Qyq8ui+vnYL5exWSrQYFkCFD6VvJoJr5ADo7CxZiyxusJM6oVHF7pA22rKJqjgIR9lksZ1+nT2WcwdXQuAFLrLFAI5L42mQKOHSx1S3vHosO0iSIX47IyyR2O+J9qLhy7B+T4cJzAq2dOtSziqL1l5BCtw5ZNYJX8N
```

The DS record for this key with digest type SHA3-256 would be:

```
example.org. IN DS 25803 8 253 BA8A4350F844CCCB8308694B3ADD478FC7EFBAC936D82D482D88F792FAB0766567E1F58F3A1075708CCC0457C9435ECA
```
8. Security considerations

8.1. Considerations for RRSIG Resource Records

DNSSEC implementations are encouraged to implement the new algorithms in this document as soon as possible now that SHA-1’s security is known to be degraded and the SHA-2 hash algorithms are currently the last line of defence for use with RSA in DNSSEC.

Users of DNS software are encouraged to deploy these new algorithms with DNSSEC when software implementations allow for it. Users are encouraged to run DNSSEC validator implementations that support these new algorithms when they are available.

The RSASSA-PSS signature scheme and the SHA-3 hash function family are considered sufficiently strong for the immediate future, but predictions about future development in cryptography and cryptanalysis are beyond the scope of this document.

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 RSASSA-PSS RRSIG and force the validator to use a RSA/SHA-1 signature if both are present in the zone. This should provide resilience against algorithm downgrade attacks, if the validator supports RSASSA-PSS.

9. IANA considerations

This document updates the IANA registry "Domain Name System Security (DNSSEC) Algorithm Numbers" (http://www.iana.org/protocols). The following entries are added to the registry:
<table>
<thead>
<tr>
<th>No.</th>
<th>Description</th>
<th>Mnemonic</th>
<th>Z.S.</th>
<th>T.S.</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>245</td>
<td>ECDSA Curve</td>
<td>ECDSAP256SHA3-256</td>
<td>Y</td>
<td>*</td>
<td>[TBD]</td>
</tr>
<tr>
<td>[TBD]</td>
<td>P-256 with SHA3-256</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>256</td>
<td>ECDSA Curve</td>
<td>ECDSAP256SHA3-384</td>
<td>Y</td>
<td>*</td>
<td>[TBD]</td>
</tr>
<tr>
<td>[TBD]</td>
<td>P-384 with SHA3-384</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>247</td>
<td>RSA/SHA2-256</td>
<td>RSASHA2-256</td>
<td>Y</td>
<td>*</td>
<td>[TBD]</td>
</tr>
<tr>
<td>[TBD]</td>
<td>with RSASSA-PSS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>248</td>
<td>RSA/SHA2-512</td>
<td>RSASHA2-512</td>
<td>Y</td>
<td>*</td>
<td>[TBD]</td>
</tr>
<tr>
<td>[TBD]</td>
<td>with RSASSA-PSS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>249</td>
<td>RSA/SHA3-256</td>
<td>RSASHA3-256</td>
<td>Y</td>
<td>*</td>
<td>[TBD]</td>
</tr>
<tr>
<td>[TBD]</td>
<td>with RSASSA-PSS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>250</td>
<td>RSA/SHA3-384</td>
<td>RSASHA3-384</td>
<td>Y</td>
<td>*</td>
<td>[TBD]</td>
</tr>
<tr>
<td>[TBD]</td>
<td>with RSASSA-PSS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>251</td>
<td>RSA/SHA3-512</td>
<td>RSASHA3-512</td>
<td>Y</td>
<td>*</td>
<td>[TBD]</td>
</tr>
<tr>
<td>[TBD]</td>
<td>with RSASSA-PSS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This document updates the IANA registry "Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms" (http://www.iana.org/protocols). The following entries are added to the registry:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Status</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>252 [TBD]</td>
<td>SHA3-256</td>
<td>OPTIONAL</td>
<td>[TBD]</td>
</tr>
<tr>
<td>253 [TBD]</td>
<td>SHA3-384</td>
<td>OPTIONAL</td>
<td>[TBD]</td>
</tr>
</tbody>
</table>

10. Acknowledgements

Thanks to Francis Dupont and Paul Hoffman for review and suggestions.

11. References

11.1. Normative references

[FIPS.180-4.2015]
National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-4, August 2015,
National Institute of Standards and Technology, "SHA-3
Standard: Permutation-Based Hash and Extendable-Output
Functions", FIPS PUB 202, August 2015,

Bradner, S., "Key words for use in RFCs to Indicate
Requirement Levels", BCP 14, RFC 2119,
DOI 10.17487/RFC2119, March 1997,

Eastlake 3rd, D., "RSA/SHA-1 SIGs and RSA KEYs in the
Domain Name System (DNS)", RFC 3110, DOI 10.17487/RFC3110,

Jonsson, J. and B. Kaliski, "Public-Key Cryptography
Standards (PKCS) #1: RSA Cryptography Specifications

Gudmundsson, O., "Delegation Signer (DS) Resource Record
(RR)", RFC 3658, DOI 10.17487/RFC3658, December 2003,

Arends, R., Austein, R., Larson, M., Massey, D., and S.
Rose, "DNS Security Introduction and Requirements",
RFC 4033, DOI 10.17487/RFC4033, March 2005,

Arends, R., Austein, R., Larson, M., Massey, D., and S.
Rose, "Resource Records for the DNS Security Extensions",
RFC 4034, DOI 10.17487/RFC4034, March 2005,

Arends, R., Austein, R., Larson, M., Massey, D., and S.
Rose, "Protocol Modifications for the DNS Security
Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005,

Hardaker, W., "Use of SHA-256 in DNSSEC Delegation Signer
(DS) Resource Records (RRs)", RFC 4509,
DOI 10.17487/RFC4509, May 2006,

Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS
Security (DNSSEC) Hashed Authenticated Denial of
11.2. Informative references


Appendix A. Change history (Editor: to be removed before publication)

- draft-muks-dnsop-dnssec-sha3-01
  Use RSASSA-PSS instead of RSASSA-PKCS1-v1_5. Specify DNSSEC algorithms using RSASSA-PSS for SHA-2 hash functions too. Specify algorithms for ECDSA with SHA-3. Update all examples. Other fixes.

- draft-muks-dnsop-dnssec-sha3-00
  Initial draft.

Authors’ Addresses

Jelte Jansen
SIDN
Meander 501
Arnhem 6825 MD
The Netherlands

Email: jelte.jansen@sidn.nl
URI: https://www.sidn.nl/