Stream:	Independent Submission
RFC:	9563
Category:	Informational
Published:	November 2024
ISSN:	2070-1721

Authors:	C. Zhang *CNNIC*	Y. Liu *CNNIC*	F. Leng *CNNIC*	Q. Zhao *CNNIC*	Z. He *CNNIC*

RFC 9563
SM2 Digital Signature Algorithm for DNSSEC

Abstract

This document specifies the use of the SM2 digital signature algorithm and SM3 hash algorithm for DNS Security (DNSSEC).

This document is an Independent Submission to the RFC series and does not have consensus of the IETF community.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9563.

Copyright Notice

Table of Contents

1. Introduction

DNSSEC is broadly defined in [RFC4033], [RFC4034], and [RFC4035]. It uses cryptographic keys and digital signatures to provide authentication of DNS data. DNSSEC signature algorithms are registered in the DNSSEC algorithm numbers registry [IANA].

This document defines the DNSKEY and RRSIG resource records (RRs) of new signing algorithms: SM2 uses elliptic curves over 256-bit prime fields with SM3 hash algorithm. (A description of SM2 can be found in GM/T 0003.2-2012 [GMT-0003.2] or ISO/IEC14888-3:2018 [ISO-IEC14888-3_2018], and a description of SM3 can be found in GM/T 0004-2012 [GMT-0004] or ISO/IEC10118-3:2018 [ISO-IEC10118-3_2018].) This document also defines the DS RR for the SM3 one-way hash algorithm. In the signing algorithm defined in this document, the size of the key for the elliptic curve is matched with the size of the output of the hash algorithm. Both are 256 bits.

Many implementations may not support SM2 signatures and SM3 digests. Section 5.2 of [RFC6840] specifies handling of answers in such cases.

Caution: This specification is not a standard and does not have IETF community consensus. It makes use of cryptographic algorithms that are national standards for China, as well as ISO/IEC standards (ISO/IEC 14888:3-2018 [ISO-IEC14888-3_2018] and ISO/IEC 10118:3-2018 [ISO-IEC10118-3_2018]). Neither the IETF nor the IRTF has analyzed that algorithm for suitability for any given application, and it may contain either intended or unintended weaknesses.

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. SM3 DS Records

The implementation of SM3 in DNSSEC follows the implementation of SHA-256 as specified in [RFC4509] except that the underlying algorithm is SM3 with digest type code 6.

The generation of an SM3 hash value is described in Section 5 of [GMT-0004] and generates a 256-bit hash value.

3. SM2 Parameters

Verifying SM2 signatures requires agreement between the signer and the verifier on the parameters used. The SM2 digital signature algorithm has been added to [ISO-IEC14888-3_2018]. The parameters of the curve used in this profile are as follows:

```
p  = FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF
     FFFFFFFF 00000000 FFFFFFFF FFFFFFFF
a  = FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF
     FFFFFFFF 00000000 FFFFFFFF FFFFFFFC
b  = 28E9FA9E 9D9F5E34 4D5A9E4B CF6509A7
     F39789F5 15AB8F92 DDBCBD41 4D940E93
xG = 32C4AE2C 1F198119 5F990446 6A39C994
     8FE30BBF F2660BE1 715A4589 334C74C7
yG = BC3736A2 F4F6779C 59BDCEE3 6B692153
     D0A9877C C62A4740 02DF32E5 2139F0A0
n  = FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF
     7203DF6B 21C6052B 53BBF409 39D54123
```

4. DNSKEY and RRSIG Resource Records for SM2

4.1. DNSKEY Resource Records

SM2 public keys consist of a single value, called "P". In DNSSEC keys, P is a string of 64 octets that represents the uncompressed form of a curve point, "x | y". (Conversion of a point to an octet string is described in Section 4.2.8 of [GM-0003.1].)

4.2. RRSIG Resource Records

The SM2 signature is the combination of two non-negative integers, called "r" and "s". The two integers, each of which is formatted as a simple octet string, are combined into a single longer octet string for DNSSEC as the concatenation "r | s". (Conversion of the integers to bit strings is described in Section 4.2.1 of [GM-0003.1].) Each integer **MUST** be encoded as 32 octets.

Process details are described in Section 6 of [GMT-0003.2].

The algorithm number associated with the DNSKEY and RRSIG resource records is 17, which is described in the IANA Considerations section.

Conformant implementations that create records to be put into the DNS **MAY** implement signing and verification for the SM2 digital signature algorithm. Conformant DNSSEC verifiers **MAY** implement verification for the above algorithm.

5. Support for NSEC3 Denial of Existence

This document does not define algorithm aliases mentioned in [RFC5155].

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

If using NSEC3, the iterations **MUST** be 0 and salt **MUST** be an empty string as recommended in Section 3.1 of [RFC9276].

6. Example

The following is an example of SM2 keys and signatures in DNS zone file format, including DNSKEY RR, NSEC3PARAM RR, NSEC3 RR with RRSIG RRs, and DS RR.

```
Private-key-format: v1.3
Algorithm: 17 (SM2SM3)
PrivateKey: V24tjJgXxp2ykscKRZdT+iuR5J1xRQN+FKoQACmo9fA=

example. 3600 IN DS 27215 17 6 (
   86671f82dd872e4ee73647a95dff7fd0af599ff8a43f fa26c9a2593091653c0e
   )

example. 3600  IN   DNSKEY  256 3 17 (
    7EQ32PTAp+1ac6R9Ze2nfB8pPc2OJqkHSjug
    ALr4SuD9awuQxhfw7wMpiXv7JK4/VwwTrCxJ
    wu+qUuDsgoBK4w==
    ) ; ZSK; alg = SM2SM3 ; key id = 65042
example. 3600  IN   RRSIG   DNSKEY 17 1 3600 (
    20230901000000 20220901000000 65042 example.
    lF2eq49e62Nn4aT5x8ZI6PdRSTPHPDixZdyl
    lM6GWu4lkRWkpTgWLE4lQK/+qHdNS4DdTd36
    Jsuu0FSO5k48Qg== )

example. 0  IN   NSEC3PARAM 1 0 10 AABBCCDD
example. 0  IN   RRSIG    NSEC3PARAM 17 1 0 (
       20230901000000 20220901000000 65042 example.
       aqntwEYEJzkVb8SNuJLwdx7f+vivv5IUIeAj )

62KP1QB93KRGR6LM7SEVPJVNG90BLUE8.example. 3600 IN NSEC3  1 1 10
    AABBCCDD (
    GTGVQIILTSSJ8FFO9J6DC8PRTFAEA8G2 NS SOA RRSIG DNSKEY NSEC3PARAM )

62KP1QB93KRGR6LM7SEVPJVNG90BLUE8.example. 3600 IN RRSIG  NSEC3 17 2
    3600 (
    20230901000000 20220901000000 65042 example.
    FOWLegTgFkFY9vCOo4kHwjEvZ+IL1NMl4s9V
    hVyPOwokd5uOLKeXTP19HIeEtW73WcJ9XNe/ ie/knp7Edo/hxw== )
```

[Example_Program] is an example program based on dnspython and gmssl, which supplies key generating, zone signing, zone validating, and DS RR generating functions for convenience.

7. IANA Considerations

IANA has registered the following in the "Digest Algorithms" registry within the "DNSSEC Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms" registry group.

Value	Digest Type	Status	Reference
6	SM3	OPTIONAL	This document

Table 1

IANA has registered the following in the "DNS Security Algorithm Numbers" registry within the "Domain Name System Security (DNSSEC) Algorithm Numbers" registry group.

Number	Description	Mnemonic	Zone Signing	Trans. Sec.	Reference
17	SM2 signing algorithm with SM3 hashing algorithm	SM2SM3	Y	*	This document

Table 2

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

8. Security Considerations

The security strength of SM2 depends on the size of the key. A longer key provides stronger security strength. The security of ECC-based algorithms is influenced by the curve it uses, too.

Like any cryptographic algorithm, it may come to pass that a weakness is found in either SM2 or SM3. In this case, the proper remediation is crypto-agility. In the case of DNSSEC, the appropriate approach would be to regenerate appropriate DS, DNSKEY, RRSIG, and NSEC3 records. Care **MUST** be taken in this situation to permit appropriate rollovers, taking into account record caching. See [RFC7583] for details. A suitable replacement algorithm should be both widely implemented and not known to have weaknesses.

The security considerations listed in [RFC4509] apply here as well.

9. References

9.1. Normative References

[GM-0003.1] Cryptography Standardization Technical Committee of China, "SM2 Public Key Cryptographic Algorithms Based on Elliptic Curves Part 1: General", [In Chinese], GM/T 0003.1-2012, March 2012. English translation available at: http://www.gmbz.org.cn/upload/2024-11-18/1731899501687024253.pdf

[GMT-0003.2] Cryptography Standardization Technical Committee of China, "SM2 Public Key Cryptographic Algorithms Based on Elliptic Curves Part 2: Digital Signature Algorithm", [In Chinese], GM/T 0003.2-2012, March 2012. English translation available at: http://www.gmbz.org.cn/upload/2024-11-18/1731899583359013934.pdf

[GMT-0004] Cryptography Standardization Technical Committee of China, "SM3 Cryptographic Hash Algorithm", [In Chinese], GM/T 0004-2012, March 2012. English translation available at: http://www.gmbz.org.cn/upload/2024-11-18/1731899426565012428.pdf.

[IANA] IANA, "DNS Security Algorithm Numbers", <https://www.iana.org/assignments/dns-sec-alg-numbers>.

[ISO-IEC10118-3_2018] ISO/IEC, "IT Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions", ISO/IEC 10118-3:2018, October 2018.

[ISO-IEC14888-3_2018] ISO/IEC, "IT Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms", ISO/IEC 14888-3:2018, November 2018.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[RFC4034] 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, <https://www.rfc-editor.org/info/rfc4034>.

[RFC4035] 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, <https://www.rfc-editor.org/info/rfc4035>.

[RFC4509] Hardaker, W., "Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)", RFC 4509, DOI 10.17487/RFC4509, May 2006, <https://www.rfc-editor.org/info/rfc4509>.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, DOI 10.17487/RFC5155, March 2008, <https://www.rfc-editor.org/info/rfc5155>.

[RFC6840] Weiler, S., Ed. and D. Blacka, Ed., "Clarifications and Implementation Notes for DNS Security (DNSSEC)", RFC 6840, DOI 10.17487/RFC6840, February 2013, <https://www.rfc-editor.org/info/rfc6840>.

[RFC7583] Morris, S., Ihren, J., Dickinson, J., and W. Mekking, "DNSSEC Key Rollover Timing Considerations", RFC 7583, DOI 10.17487/RFC7583, October 2015, <https://www.rfc-editor.org/info/rfc7583>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC9276] Hardaker, W. and V. Dukhovni, "Guidance for NSEC3 Parameter Settings", BCP 236, RFC 9276, DOI 10.17487/RFC9276, August 2022, <https://www.rfc-editor.org/info/rfc9276>.

9.2. Informative References

[Example_Program] "sign and validate dnssec signature with sm2sm3 algorithm", commit 6f98c17 , April 2023, <https://github.com/scooct/dnssec_sm2sm3>.

Authors' Addresses

Cuiling Zhang
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing
100190
China
Email: zhangcuiling@cnnic.cn

Yukun Liu
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing
100190
China
Email: liuyukun@cnnic.cn

Feng Leng
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing
100190
China
Email: lengfeng@cnnic.cn

Qi Zhao
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing
100190
China
Email: zhaoqi@cnnic.cn

Zheng He
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing
100190
China
Email: hezh@cnnic.cn