Workgroup: Network Working Group
Internet-Draft: draft-cuiling-dnsop-sm2-alg-00
Updates: 8624 (if approved)
Published: 2022-04-07
Intended Status: Informational
Expires: 2022-10-07

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

SM2 Digital Signature Algorithm for DNSSEC

Abstract

This document describes how to specify SM2 Digital Signature Algorithm keys and signatures in DNS Security (DNSSEC). It lists the curve and uses SM3 as hash algorithm for signatures.

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 https://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 xx xxx 2022.

1. Introduction

DNSSEC is broadly defined in RFCs 4033, 4034, and 4035 ([RFC4033],

[RFC4034], and [RFC4035]). It uses cryptographic keys and digital signatures to provide authentication of DNS data. Currently, there are several signature algorithms, such as RSA with SHA-256,ECDSA with curve P-256 and SHA-256, etc.

This document defines the DNSKEY and RRSIG resource records (RRs) of a new signing algorithms: SM2 uses elliptic curves over 256-bit prime fields with SM3 hash algorithm. (A description of SM2 and SM3 can be found in ISO/IEC 10118-3:2018 [ISO/IEC10118-3:2018] and ISO/IEC 14888-3:2018 [ISO/IEC14888-3:2018].) 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.

Like all ECC-based algorithms, signing with SM2 is significantly faster than RSA based algorithms, while the validating is slower.

Due to the similarity between SM2 and ECDSA with curve P-256, some of the material in this document is copied liberally from RFC 6605 [RFC6605].

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 RFC 2119 [RFC2119].

2. SM3 DS Records

SM3 is included in ISO/IEC 10118-3:2018 and is similar to SHA-256 in many ways. The implementation of SM3 in DNSSEC follows the implementation of SHA-256 as specified in RFC 4509[RFC4509] except that the underlying algorithm is SM3, the digest value is 32 bytes long, and the digest type code is 17 [to be determined].

3. SM2 Parameters

Verifying SM2 signatures requires agreement between the signer and the verifier of the parameters used. SM2 digital signature algorithm has been added to ISO/IEC 14888-3:2018. And the parameters of the curve used in this document 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

SM2 public keys consist of a single value, called "P". In DNSSEC keys, P is a simple bit string that represents the uncompressed form of a

curve point, "x | y".

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 the same as ECDSA signature.) Each integer MUST be encoded as 32 octets.

Although SM2 uses elliptic curves, the process of digest and signature generation is different from ECDSA.

The algorithm number associated with the DNSKEY and RRSIG resource records is fully defined in the IANA Considerations section. It is:

DNSKEY and RRSIG RRs signifying SM2 with SM3 use the algorithm number 17 [to be determined].

Conformant implementations that create records to be put into the DNS MAY implement signing and verification for the above 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 RFC 5155 [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 1, as defined in RFC 5155. 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.

6. Example

The following is an example of SM2 keys and signatures in DNS format.

6.1. SM2 Example

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

example.net. 3600 IN DNSKEY 257 3 17 (
  jZbZMBImG9dtGWSVEwnv2l32OVKcX7MMJv+83/+A41ia
  ZuO0ajXMcuyJbTr8Ud+kae6UlfqrnsG6tgADIPHxXA== )

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

www.example.net. 3600 IN A 192.0.2.1
```

```
www.example.net. 3600 IN RRSIG A 17 6 3600 (
  20220428075649 20220331075649 27215 example.net.
  tz295lkfu2InRnLdLhKWDm354I6ZGSmYeOSDswKiQMU7
  /Va0QrH7bD7ZnHB4wWsEjfy1XscwM4P86sVxkMJE7w== )
```

7. IANA Considerations

This document updates the IANA registry for digest types in DS records, currently called "Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms". The following entry has been added:

Value	6 [to be determined]
Digest Type	SM3
Status	OPTIONAL

This document updates the IANA registry "Domain Name System Security (DNSSEC) Algorithm Numbers". The following two entries have been added to the registry:

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

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

8. Security Considerations

The cryptographic work factor of SM2 is generally considered to be equivalent to half the size of the key, which is 128 bits. Such an assessment could, of course, change in the future if new attacks that work better than the ones known today are found.

SM2 digital signature algorithm has come into use for less than a score of years. So SM2SM3 algorithm is mainly used for research and experiment purpose currently.

The security considerations listed in RFC 4509 apply here as well.

9. Normative References

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

[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.

[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.

[RFC6605] Hoffman, P., and Wouter C.A. Wijngaards, "Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC", RFC 6605, April 2012.

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

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

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