ICS 35.100.70
CCS L79

团 体 标 准

T/CCSA 563—2024

域名服务系统安全扩展（DNSSEC）支持SM2/SM3算法的技术要求

Technical requirement of DNSSEC with ShangMi (SM) cipher suites

2024－11－11 发布　　2025－01－01 实施

中国通信标准化协会　　发 布

版权声明

目　　次

前言 II
引言 III
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　缩略语 1
5　DNSSEC 相关资源记录的表示方法 1
5.1　扩展算法对 DNSSEC 资源记录的影响 1
5.2　DNSKEY 资源记录 2
5.3　RRSIG 资源记录 2
5.4　DS 资源记录 2
6　DNS 数据签名的计算和验证 2
6.1　密钥文件的格式及表示方法 2
6.2　计算签名 2
6.3　验证签名 3
附录 A（资料性）　使用 SM2/SM3 算法的 DNSSEC 密钥文件示例 4
A.1　私钥文件 4
A.2　公钥文件 4
附录 B（资料性）　使用 SM2/SM3 算法的 DNSSEC 权威域区文件示例 5
附录 C（资料性）　使用 SM2/SM3 算法生成及验证 RRSIG 资源记录示例 8
C.1　RRSIG 资源记录生成步骤范例 8
C.2　RRSIG 资源记录验证步骤范例 8
参考文献 9

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：中国互联网络信息中心、中国信息通信研究院、中国信息通信科技集团有限公司、郑州信大捷安信息技术股份有限公司、北京首信科技股份有限公司。

本文件主要起草人：张翠玲、刘昱琨、冷峰、何峥、赵琦、陈涛、刘为华、袁琦、梅秋丽。

引　言

为适应信息通信业发展对标准文件的需求，由中国通信标准化协会组织制定“中国通信标准化协会团体标准”，推荐有关方面采用。有关对本标准的建议和意见，向中国通信标准化协会反映。

域名服务系统安全扩展（DNSSEC）支持 SM2/SM3 算法的技术要求

1 范围

本文件规定了在域名服务系统安全扩展（DNSSEC）协议中使用SM2数字签名算法和SM3密码杂凑算法的技术要求，包括DNSSEC相关资源记录（公钥记录、签名记录、摘要记录）格式及含义，DNS数据签名计算和验证方法等内容。

本文件适用于指导在DNSSEC中使用SM2/SM3算法对DNS数据进行签名和验证。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 32905-2016信息安全技术 SM3密码杂凑算法

GB/T 32918.2-2016信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法

GB/T 32918.5-2017信息安全技术 SM2椭圆曲线公钥密码算法 第5部分：参数定义

GB/T 36619-2018 信息安全技术政务和公益机构域名命名规范 术语

YD/T 2586-2013 DNSSEC协议和实现要求 术语

IETF RFC 4034 资源记录支持DNSSEC 的扩展（Resource Records for the DNS Security Extensions）

3 术语和定义

GB/T 36619-2018和YD/T 2586-2013界定的以及下列术语和定义适用于本文件。

3.1

域名 domain name

互联网络上识别和定位计算机的层次结构式的字符标识，与该计算机的互联网协议（IP）地址相对。一般英文域名由英文字母、数字及连字符（“-”）等ASCII编码组成，国际化域名（IDN）由非ASCII编码的字符组成，比如“.中国”，“.公司”等。

[来源：GB/T 36619-2018，定义3.1]

4 缩略语

下列缩略语适用于本文件。

DNS：域名系统（Domain Name System）

DNSKEY：域名系统公钥（DNS Public Key）

DNSSEC：域名系统安全扩展（Domain Name System Security Extensions）

DS：授权签名者（Delegation Signer）

NSEC：下一个安全记录（Next Secure）

NSEC3：下一个安全记录第三版（Next Secure Version 3）

RRSIG：资源记录签名（Resource Record Signature）

TTL：生存时间（Time To Live）

5 DNSSEC 相关资源记录的表示方法

5.1 扩展算法对 DNSSEC 资源记录的影响

DNSSEC的提出引入RRSIG、DNSKEY、DS、NSEC/NSEC3等新资源记录类型。本文件仅涉及SM2/SM3算法在RRSIG、DNSKEY及DS三种资源记录中的表示方法，未对NSEC/NSEC3资源记录所使用的算法进行扩展。

5.2 DNSKEY 资源记录

DNSKEY资源记录的报文包括16比特的标志位（Flags），8比特的协议字段（Protocol），8比特的算法字段（Algorithm）和公钥字段（Public Key）。其中算法字段和公钥字段的内容与所使用的数字签名算法有关。

算法字段为17，表示SM2算法。

公钥字段保存权威域公钥，使用SM2算法生成的公钥字段格式定义如下：

公钥字段长度为512比特，由SM2算法中公钥P(xP,yP)的x坐标xP和y坐标yP连接而成。算法所使用的椭圆曲线参数遵从GB/T 32918.5-2017中规定。

5.3 RRSIG 资源记录

RRSIG资源记录的报文包括16比特的类型覆盖字段(Type Covered)、8比特的算法字段(Algorithm)、8比特的域名字段字段（Labels）、32比特的原始生命周期字段（Original TTL）、32比特的签名过期时间字段（Signature Expiration）、32比特的签名开始时间字段（Signature Inception）、16比特的密钥标签字段（Key Tag）、签名者字段（Signer’s Name）和签名字段（Signature）。其中算法字段和签名字段的内容与所使用的数字签名算法有关。

算法字段为17，表示SM2算法。

签名字段保存资源记录集的数字签名，使用SM2算法生成的签名字段格式定义如下：

签名字段长度为512比特，由SM2算法中签名(r,s)的两个非负整数r和s连接而成。每个整数表示为256位比特串。

5.4 DS 资源记录

DS资源记录的报文包括16比特的密钥标签字段（Key Tag）、8比特的算法字段（Algorithm）、8比特的散列类型字段（Digest Type）和散列值字段（Digest）。其中算法字段与对应DNSKEY资源记录的算法字段一致。散列类型字段和散列值字段与所使用的散列算法有关。

散列类型字段为6，表示SM3算法。

散列值字段保存权威域公钥散列值，使用SM3算法生成的散列值字段格式定义如下：

散列值字段长度为256比特，生成方法遵从GB/T 32905-2016中规定。

6 DNS 数据签名的计算和验证

6.1 密钥文件的格式及表示方法

计算RRSIG资源记录签名字段时，需使用SM2算法的私钥。

SM2算法私钥长度为256比特，宜以BASE64编码形式表示，可保存在私钥文件中，不可在DNS系统中公开。私钥文件范例可参见附录A中A.1。

SM2算法公钥长度为512比特，应以BASE64编码形式在区数据中发布。公钥文件范例可参见附录A中A.2。

SM2算法采用Fp-256曲线，曲线参数遵从GB/T 32918.5-2017的规定。

6.2 计算签名

DNS服务器在计算DNS数据签名时，需要根据DNS数据构造签名前数据，然后使用SM2算法私钥计算数字签名。其中签名前数据、私钥、签名的含义如下：

a) 签名前数据（输入参数）：以资源记录集为单位，构造签名前数据。具体构造格式可参见 RFC 4034；
b) 私钥（输入参数）：SM2 算法使用的私钥；
c) 签名（输出参数）：使用 SM2 算法计算出的数字签名，保存于 RRSIG 资源记录中，包含算法号、DNSKEY 密钥标签、签名等信息。RRSIG 资源记录范例可参见附录 B；

d) 计算签名的方法为：使用私钥根据 GB/T 32918.2-2016 中计算签名的方法，生成数字签名，并以 RRSIG 资源记录的形式保存于区数据中。计算签名步骤范例可参见附录 C 中 C.1。

6.3 验证签名

DNS客户端在验证DNS数据签名时，需要根据DNS数据构造签名前数据，然后使用SM2算法公钥对签名数据进行验证。其中签名前数据、公钥、签名的含义如下：

a) 签名前数据（输入参数）：同 6.2 中签名前数据；
b) 公钥（输入参数）：SM2 算法使用的公钥以 DNSKEY 资源记录的形式保存于区数据中。DNSKEY 资源记录范例可参见附录 B；
c) 签名（输入参数）：同 6.2 中签名；
d) 验证签名的方法为：使用 DNSKEY 资源记录中的公钥，根据 GB/T 32918.2-2016 中验证签名的方法，对 RRSIG 资源记录中签名进行验证。验证结果为通过或不通过。验证签名步骤范例可参见附录 C 中 C.2。

附 录 A
（资料性）
使用 SM2/SM3 算法的 DNSSEC 密钥文件示例

本附录为使用SM2/SM3算法的DNSSEC密钥文件示例。

A.1 私钥文件

一个保存私钥d的文件Kexample.+017+27215.private范例如下：

```
Private-key-format: v1.3
Algorithm: 17 (SM2SM3)
PrivateKey: V24tjJgXxp2ykscKRZdT+iuR5J1xRQN+FKoQACmo9fA=
Created: Mon Apr 10 16:23:43 2023
Publish: Mon Apr 10 16:23:43 2023
Activate: Mon Apr 10 16:23:43 2023
```

其中PrivateKey字段是256比特整数私钥d的BASE64编码形式。

A.2 公钥文件

一个保存公钥P的文件Kexample.+017+27215.key范例如下：

```
; This is a key-signing key, keyid 27215, for example.
; Created: Mon Apr 10 16:23:42 2023 (20230410162342)
; Publish: Mon Apr 10 16:23:42 2023 (20230410162342)
; Activate: Mon Apr 10 16:23:42 2023 (20230410162342)
example. IN DNSKEY 257 3 17 jZbZMBImG9dtGWSVEwnv2l32OVKcX7MMJv+83/+A41iaZuO0ajXMcuyJb
Tr8Ud+kae6UlfqrnsG6tgADIPHxXA==
```

附 录 B
（资料性）
使用 SM2/SM3 算法的 DNSSEC 权威域区文件示例

一个完整的使用SM2/SM3算法的DNSSEC权威域区文件示例如下：

```
example. 3600    IN      SOA       ns1.example. root.example. (
                                   1             ; serial
                                   3600          ; refresh (1 hour)
                                   300           ; retry (5 minutes)
                                   3600000       ; expire (5 weeks 6 days 16 hours)
                                   3600          ; minimum (1 hour)
                                   )
                         RRSIG     SOA 17 1 3600 (
                                   20251215000000 20231215000000 65042 example.
                                   MymnmMCQG3R/sMxTmQRD7yAvpVefMUjN34we
                                   x8WOy4+vpDitAFFSjhnYjO4uqZkcKUphfRJa
                                   /VLVyX++e/+r3w== )
                         NS        ns1.example.
                         NS        ns2.example.
                         RRSIG     NS 17 1 3600 (
                                   20251215000000 20231215000000 65042 example.
                                   L2Jgy38wJZdh6o1PTg0tCyqIwO4ieQNRW5Fb
                                   TvK0dB/UNf46tD9bUMY40xaxgnxuNui7HPXp
                                   5u6cZi49DOZe9w== )
                         DNSKEY    256 3 17 (
                                   7EQ32PTAp+1ac6R9Ze2nfB8pPc2OJqkHSjug
                                   ALr4SuD9awuQxhfw7wMpiXv7JK4/VwwTrCxJ
                                   wu+qUuDsgoBK4w==
                                   ) ; ZSK; alg = SM2SM3 ; key id = 65042
                         DNSKEY    257 3 17 (
                                   jZbZMBImG9dtGWSVEwnv2l32OVKcX7MMJv+8
                                   3/+A41iaZuO0ajXMcuyJbTr8Ud+kae6Ulfqr
                                   nsG6tgADIPHxXA==
                                   ) ; KSK; alg = SM2SM3 ; key id = 27215
                         RRSIG     DNSKEY 17 1 3600 (
                                   20251215000000 20231215000000 27215 example.
                                   imSG2QZDq7ua38EkSPuzZ9mujsMbAO5B058o
                                   3KXYyOzcqaR1IhVARkgTIGqeigzAHh93ba/m
                                   IB1bgQcNgLYMgQ== )
                         RRSIG     DNSKEY 17 1 3600 (
                                   20251215000000 20231215000000 65042 example.
                                   T4OuEqHAoeX7jhF6Fv0/47o+qQ+zZghDBbSU
                                   99vb1EYj01ODkXGNz3YGgN+SH96wq608DSsi
                                   f1ri2i4lHSPNxw== )
                   0     NSEC3PARAM 1 0 0 -
                   0     RRSIG       NSEC3PARAM 17 1 0 (
                                   20251215000000 20231215000000 65042 example.
                                   +kD6n8D8DcqQDQXa0m9zUAbWjZ6R6jU2vcov
                                   0rvZTKOwDFJqvu/fobA0taD5ugnFah9TEUna
                                   ZNIMSuLtDYTb/g== )
child.example. 3600 IN NS ns1.child.exmple.
child.example. 3600 IN NS ns2.child.exmple.
                         RRSIG     NS 17 2 3600 (
```

```
                    20251215000000 20231215000000 65042 example.
                    1waowbu4LdNfkzFd/4G4NuJaH6uS1m39jeBR
                    bSBBqHVV0EkzfSUPKrcWP/5WeiVz2QU32Ayb
                    g32c6VjjgPBjpw== )
child.example.      DS     6400 17 6
                    4236D83078C14118A9396275229F7161699B05460B32D9447BF64437
                    94BA8BBF
                RRSIG  DS 17 2 3600 (
                    20251215000000 20231215000000 65042 example.
                    TZNtaAOmHLqwRrV2O1/gztAm3MSSdtg4zQ0j
                    xzJuuPzhYXbDXh8lUgRx2UTsLrKIDkeNr+Jq
                    /f6/9tcnD66Xmg== )
ns1.child.example.  IN A        192.0.3.1
ns2.child.example.  IN A        192.0.3.2
ns1.example.    A   192.0.2.1
                RRSIG  A 17 2 3600 (
                    20251215000000 20231215000000 65042 example.
                    jTGyiOV6s3A1JVFCl+HaZ4T5IHErL/IPac28
                    3aE+tK+R4sWCjmG+aobpinaD18dTijCTBsZ5
                    DFIk8YNV/d+hMg== )
ns2.example.    A   192.0.2.2
                RRSIG  A 17 2 3600 (
                    20251215000000 20231215000000 65042 example.
                    Kkj7OF/M/n9rY1eUVKnr66mWHdoXbR3pZ2jU
                    WmpCfVdPM9s713llGeyOZ3ObWidFb+haOpni
                    NYqMgsmeINz0+Q== )
test.example.   A   192.0.2.4
                RRSIG  A 17 2 3600 (
                    20251215000000 20231215000000 65042 example.
                    1x9q3Y1LxfEaw8UJgtIBfI8AXyGjPXW+tyhu
                    n4GHjuu3VlTabIS5rUQATu7q2XGtRrO8mibd
                    pL72NUKlydU2VA== )
www.example.    A   192.0.2.3
                RRSIG  A 17 2 3600 (
                    20251215000000 20231215000000 65042 example.
                    KxDUkb/UUPtDzb8puRnMcLyF9in4t2eiykx2
                    t0Ofob9GtPbxZiDPndtEB7LK2HpdHyE8BHfi
                    9l3fBy76KKZhUA== )
3MSEV9USMD4BR9S97V51R2TDVMR9IQO1.example.  NSEC3  1 0 0 - (
                    9BTQ22OI7FGU6V6RMM87HRIUTRT6ERVD
                    NS SOA RRSIG DNSKEY NSEC3PARAM )
                RRSIG  NSEC3 17 2 3600 (
                    20251215000000 20231215000000 65042 example.
                    3iLUxUDH3BzAVlk1MN+TuHkybdAixJwZfTer
                    pRmOzAUfDTpVNFKaXBEFJvb3OWNCZDwkLeeB
                    c7n35ZGMVhcLyw== )
9BTQ22OI7FGU6V6RMM87HRIUTRT6ERVD.example.  NSEC3  1 0 0 - (
                    9KQNRPNEKPLBCT2M3K9JH3CLJVIOK2B5
                    NS DS RRSIG )
                RRSIG  NSEC3 17 2 3600 (
                    20251215000000 20231215000000 65042 example.
                    VAKk9wBAyBaM0KMsIVQZqIEMjbWR2Ga5vduO
                    My0IGwinqzgcKvPG0z7Dx3qUU1xsKuVGaKTB
                    fceQMccqLM1j0Q== )
9KQNRPNEKPLBCT2M3K9JH3CLJVIOK2B5.example.  NSEC3  1 0 0 - (
                    CKB3499RRJ8EBL601LHFLJCHMLJ45RJV
```

```
                A RRSIG )
        RRSIG   NSEC3 17 2 3600 (
                20251215000000 20231215000000 65042 example.
                FRqQg6V3jRvxMbjRxF7hsQJN6kjD+XRa5NC9
                l4XDCYCEUhQ0vzgwHNA7FnRDNYWb7k28wJEF
                iJaAEPM9LEKT/g== )
CKB3499RRJ8EBL601LHFLJCHMLJ45RJV.example.  NSEC3 1 0 0 - (
                DSQ717D99RRRN3N4O1O20NTK5LDJKNT3
                A RRSIG )
        RRSIG   NSEC3 17 2 3600 (
                20251215000000 20231215000000 65042 example.
                tXyfFd686SHz/hvOdKjMaqNhPSodN5K5OF/2
                yPg5tB8gbb9JgZlgpmMj+cwmee1k+mPgw8VF
                nxk5AVbR+c4ylA== )
DSQ717D99RRRN3N4O1O20NTK5LDJKNT3.example.  NSEC3  1 0 0 - (
                M1O89LFDO9RRF2F8R8SS42D81D09V48M
                A RRSIG )
        RRSIG   NSEC3 17 2 3600 (
                20251215000000 20231215000000 65042 example.
                4mO9NlkUDLMnrH6W86XL3/4hIqXu8Fbj/mha
                SzRLNu1DNSs2wL03knfG94wvTna855kq+wPV
                c2MObyEOyru0pw== )
M1O89LFDO9RRF2F8R8SS42D81D09V48M.example.  NSEC3  1 0 0 - (
                3MSEV9USMD4BR9S97V51R2TDVMR9IQO1
                A RRSIG )
        RRSIG   NSEC3 17 2 3600 (
                20251215000000 20231215000000 65042 example.
                xzL10PXumEegAHqxYJ5D7PoDQH2Mo1RHIXTW
                xtyN3U299BKhVN2Nbc0VFWhy4Z/ILVsSG8kq
                GVk7//4LkU+Gbw== )
```

附 录 C
（资料性）
使用 SM2/SM3 算法生成及验证 RRSIG 资源记录示例

本附录为使用SM2/SM3签名算法生成及验证RRSIG资源记录的示例。

C.1 RRSIG 资源记录生成步骤范例

步骤如下：

a） **构造签名前数据：**签名前数据：以下述资源记录集为例，包含 2 条 DNSKEY 类型的资源记录。

example. 3600 IN DNSKEY 256 3 17 (7EQ32PTAp+1ac6R9Ze2nfB8pPc2OJqkHSjug
ALr4SuD9awuQxhfw7wMpiXv7JK4/VwwTrCxJ
wu+qUuDsgoBK4w==)
example. 3600 IN DNSKEY 257 3 17 (jZbZMBImG9dtGWSVEwnv2l32OVKcX7MMJv+8
3/+A41iaZuO0ajXMcuyJbTr8Ud+kae6Ulfqr
nsG6tgADIPHxXA==)

根据 RFC 4034 关于 RRSIG 资源记录中签名前数据的构造格式，以十六进制表示为：

0x00300d0100000e1064f12980630ff6006a4f076578616d706c6500076578616d706c650000300000100000e1000440100030dec4437d8f4c0a7ed5a73a47d65eda77c1f293dcd8e26a9074a3ba000baf84ae0fd6b0b90c617f0ef0329897bfb24ae3f570c13ac2c49c2efaa52e0ec82804ae3076578616d706c650000300001000000e1000440101030d8d96d93012261bd76d1964951309efda5df639529c5fb30c26ffbcdfff80e3589a66e3b46a35cc72ec896d3afc51dfa469ee9495faab9ec1bab6000320f1f15c

b） **使用私钥计算 DNS 数据签名：**私钥通常保存于密钥文件中，其 BASE64 格式为：

V24tjJgXxp2ykscKRZdT+iuR5J1xRQN+FKoQACmo9fA=

表示为十六进制格式为：

0x576e2d8c9817c69db292c70a459753fa2b91e49d7145037e14aa100029a8f5f0

使用私钥计算出的签名，以十六进制表示为：

0xf8c0c5d5b9c7ffccc278ec0941b5927f06fa38207c7e9d7aaf1a204bdf8f6f11c470a3533945f784fc5d33c35b943818d7d73e2839abc5e8b60fce0cd81e7471

其 BASE64 格式如下：

+MDF1bnH/8zCeOwJQbWSfwb6OCB8fp16rxogS9+PbxHEcKNTOUX3hPxdM8NblDgY19c+KDmrxei2D84M2B50cQ==

c） **生成 RRSIG 资源记录：**根据 5.3 中 RRSIG 资源记录定义，生成如下记录：

example. 3600 IN RRSIG DNSKEY 17 1 3600 (
20230901000000 20220901000000 27215 example.
+MDF1bnH/8zCeOwJQbWSfwb6OCB8fp16rxog
S9+PbxHEcKNTOUX3hPxdM8NblDgY19c+KDmr
xei2D84M2B50cQ==)

C.2 RRSIG 资源记录验证步骤范例

步骤如下：

a） **构造签名前数据：**签名前数据构造方法同 C.1。

b） **使用公钥验证 RRSIG 资源记录：**公钥保存于 DNSKEY 资源记录中，其 BASE64 格式为：

jZbZMBImG9dtGWSVEwnv2l32OVKcX7MMJv+83/+A41iaZuO0ajXMcuyJbTr8Ud+kae6UlfqrnsG6tgADIPHxXA==

签名保存于 RRSIG 资源记录中，其 BASE64 格式为：

+MDF1bnH/8zCeOwJQbWSfwb6OCB8fp16rxogS9+PbxHEcKNTOUX3hPxdM8NblDgY19c+KDmrxei2D84M2B50cQ==

使用公钥对签名进行验证，如果验证通过，则 RRSIG 资源记录验证通过；反之，验证不通过。

此范例验证结果为通过。

参 考 文 献

[1] GB/T 36619-2018 《信息安全技术政务和公益机构域名命名规范》
[2] GB/T 32918.2-2016 《信息安全技术 SM2 椭圆曲线公钥密码算法 第 2 部分：数字签名算法》
[3] GB/T 32918.5-2017 《信息安全技术 SM2 椭圆曲线公钥密码算法 第 5 部分：参数定义》
[4] GB/T 32905-2016 《信息安全技术 SM3 密码杂凑算法》
[5] YD/T 2586-2013 《DNSSEC 协议和实现要求》
[6] IETF RFC 4034 Resource Records for the DNS Security Extensions