高技术通讯 2026 年 第36卷 第5期:478 – 488

doi:10.3772/j.issn.1002 – 0470.2026.05.004

基于 SM2SM3 算法的域名系统安全扩展应用研究①

张翠玲② 孙 琪 何 峥③ 唐洪峰 姜郁峰 李帅良 李汉明

(中国互联网络信息中心 北京 100070)

摘 要 域名系统(domain name system, DNS)作为互联网的基础设施,负责将人类可读的域名转换为机器可读的互联网协议(Internet protocol,IP)地址。然而,传统的 DNS 协议在设计时并未充分考虑安全性,容易受到诸如缓存投毒、中间人攻击等安全威胁。域名系统安全扩展(DNS security extensions, DNSSEC)通过引入数字签名机制,确保 DNS 响应的完整性和真实性,能够有效提升 DNS 系统的安全性,从而有效防止这些攻击。DNSSEC 支持多种密码算法,RFC(request for comments)9563 规定了在 DNSSEC 中使用 SM2SM3 算法的公钥记录、签名记录格式以及算法号。为推广国家商用密码(Shang Mi,SM)算法在 DNSSEC 领域的应用,本文对基于 SM2SM3 算法的 DNSSEC 应用关键问题进行了分析研究并提出解决方案。

关键词 域名系统;域名系统安全扩展;域名系统安全扩展签名算法替换;SM 系列密码算法

域名系统(domain name system,DNS)作为互联网基础设施的核心组成部分,承担着将人类可读的域名转换为机器可读的 IP 地址的重要功能。然而,传统的 DNS 协议在设计之初并未充分考虑安全性,导致其容易受到多种网络攻击的威胁。域名系统安全扩展(DNS security extensions,DNSSEC)[1-3]通过引入数字签名和公钥基础设施(public key infrastructure,PKI)机制,为 DNS 响应提供了数据完整性验证和来源认证,从而有效防止 DNS 数据被篡改或伪造。

近年来,我国国产密码算法技术不断发展与推广,已在通信、交通、能源等关键领域实现了深度应用。以工业互联网安全领域为例,国密算法在身份认证、访问控制、账户管理以及数据安全等多个方面发挥了至关重要的作用[4]。同时,在城市轨道交通综合监控系统中,国密算法也被成功应用于系统认证、通信加密及存储加密等核心环节,有效提升了系统的安全性[5]。此外,国密算法还应用于智能电表安全芯片的设计中[6],为电力行业的安全稳定运行提供了有力保障。不仅如此,国密算法的应用还拓展至资源公钥基础设施(resource public key infrastructure,RPKI)证书的签发[7],以及智能家居服务端与网关设备端的身份认证与传输数据加密等方面[8],进一步体现了其应用潜力和应用前景。我国商用密码(Shang Mi,SM)算法——SM2 数字签名算法及 SM3 杂凑密码算法于 2018 年分别被纳入 ISO/IEC 14888-3∶2018 及 ISO/IEC 10118-3∶2018(ISO:International Organization for Standardization;IEC:International Electrotechnical Commission),正式成为国际标准,标志着我国密码算法国际标准体系已初步成形。

从算法所能提供的安全等级维度来看,SM2 算法的安全级别与基于 256 位密钥长度的椭圆曲线加密(elliptic curve cryptography,ECC)算法相当[9]。同时,依据美国国家标准与技术研究院(National Institute of Standards and Technology,NIST)发布的密钥管理建议所提供的数据,ECC 算法 256 位密钥长

① 国家重点研发计划(2022YFB3103000)和中国互联网络信息中心自立科研项目(Z24020805)资助。
② 女,1982 年生,硕士,高级工程师;研究方向:域名系统运行与安全;E-mail:zhangcuiling@cnnic.cn。
③ 通信作者,E-mail:hezheng@cnnic.cn。
(收稿日期:2025 – 05 – 13)

度所具备的安全级别,与 RSA(Rivest-Shamir-Adleman)算法 3 072 位密钥长度的安全级别处于同一水准[10]。因此 SM2 算法的安全级别与 RSA 算法 3 072 位密钥长度的安全级别相仿。

随着新通用顶级域的推广,DNSSEC 的全球部署率正在逐步提高。目前 DNSSEC 已支持 10 余种密码算法,随着密码学的发展,使用安全性更好的新算法替换旧算法非常重要。一项算法在 DNSSEC 中的生命周期包括标准化、软件支持、运维部署和弃用 4 个阶段,这一过程的便捷程度被称为算法的敏捷性[11]。因此标准化、软件支持和运维部署是在 DNSSEC 中推广部署 SM2/SM3 算法的关键问题。2024 年发布的 RFC(request for comments) 9563 规定了在 DNSSEC 中使用 SM2SM3 算法的公钥记录、签名记录格式以及算法号,有效解决了 DNSSEC 应用的互联互通问题,完成了算法标准化的工作,为下一步软件支持及运维部署打下了基础。

本文旨在探讨在 DNSSEC 中推广部署 SM2SM3 算法的关键问题及其解决方案,为推广我国商密算法在 DNSSEC 领域的应用提供更为广阔和深入的视角,具有重要的研究与指导意义。本文首先对解析软件和解析服务提供商进行了调研分析,总结其对 DNSSEC 签名算法的支持情况,以及所依赖的安全软件库,为下一步支持 SM2SM3 算法提供基础。随后,本文提出了一种从其他已有 DNSSEC 算法变更为 SM2SM3 算法的迁移方案,对迁移过程中信任链变化过程进行分析,论证并验证其保证业务连续性实现算法平滑过渡的可行性。这种方法不仅适用于从其他 DNSSEC 算法迁移为 SM2SM3 算法的场景,也普遍适用于任意 2 种不同算法的迁移过程,有助于提升 DNSSEC 算法的敏捷性,降低新算法部署环节的风险性。

本文的主要贡献如下。

(1) 通过对行业主流解析软件及服务提供商对 DNSSEC 签名算法的支持情况进行调研分析,提出软件层面支持 SM2SM3 算法的解决方案。本文对 ISC BIND、NSD/Unbound、Knot DNS 等软件,及 Cloudflare、阿里、腾讯等云解析服务厂商对 DNSSEC 签名算法的支持情况进行总结,并对软件所依赖的安全软件库进行了调研,提出了推动软件层面支持 SM2SM3 算法的解决方案,为解析软件及服务对算法的支持提供了方向和指导。

(2) 论证从其他已有 DNSSEC 算法变更为 SM2SM3 算法的迁移方案的可行性。本文根据 RFC 6781[12] 中的算法轮转步骤,形成算法迁移方案,并对方案可行性进行了理论分析与实验验证。通过对迁移过程中各阶段信任链状态的分析以及实验模拟,论证了迁移方案的可行性。

1 背 景

1.1 域名系统的层次结构

域名系统的层次结构呈倒置的树形,自顶向下为根域名服务器、顶级域名服务器和其他权威服务器,权威服务器提供有关特定域名的权威性答案[13]。此外还包含递归服务器,负责处理用户的查询请求并在必要时将请求传递给其他服务器。查询域名关联数据(如互联网协议(Internet procotol,IP)地址)的过程称为域名解析。

1.2 DNSSEC 原理

DNSSEC 协议是针对 DNS 协议的安全扩展,其架构类似公钥基础设施(Public Key Infrastructure,PKI)。通过为 DNS 数据添加基于非对称加密算法的数字签名,以保证数据未经篡改。通过向父区提交公钥记录的摘要,实现域名体系的逐级安全认证。客户端在得到应答消息后,可以通过检查此签名信息来判断应答数据的完整性和真实性,从而防止针对 DNS 的相关攻击。

DNSSEC 引入 4 种新 DNS 资源记录(resource record,RR),其中 3 种用于信任链的验证,分别为 DNS 公钥(DNS public key,DNSKEY)记录、资源记录签名(resource record signature,RRSIG)记录和委托签名者(delegation signer,DS)记录。

DNSKEY 记录存储指定区的公钥,包括签名算法和公钥等字段。DNSSEC 中的密钥分为区签名密钥(zone signing key,ZSK)和密钥签名密钥(key signing key,KSK),分别用于对区数据和 DNSKEY 记录的签名。如无特别说明,文中 DNSKEY 同时包括 KSK 及 ZSK。

RRSIG 记录存储指定资源记录集的签名，包括签名算法、密钥标签（Key Tag）和签名等字段。其中签名算法字段与对应的 DNSKEY 记录签名算法字段一致，密钥标签字段由公钥计算得出，验证签名时，可帮助快速确定对应的 DNSKEY 记录。

DS 记录存储 KSK 公钥的摘要，包括密钥标签、签名算法、摘要算法和摘要等字段。其中密钥标签由 KSK 的公钥计算得出，签名算法字段与 DNSKEY 记录中的签名算法字段一致。

DNSSEC 信任链示意如图 1 所示。DNSKEY 记录和 RRSIG 记录位于子区，用于对子区数据的验证；DS 记录位于父区，用于对子区 KSK 公钥的验证。信任链验证的终点为信任锚，通常设置为根区的 KSK 记录。

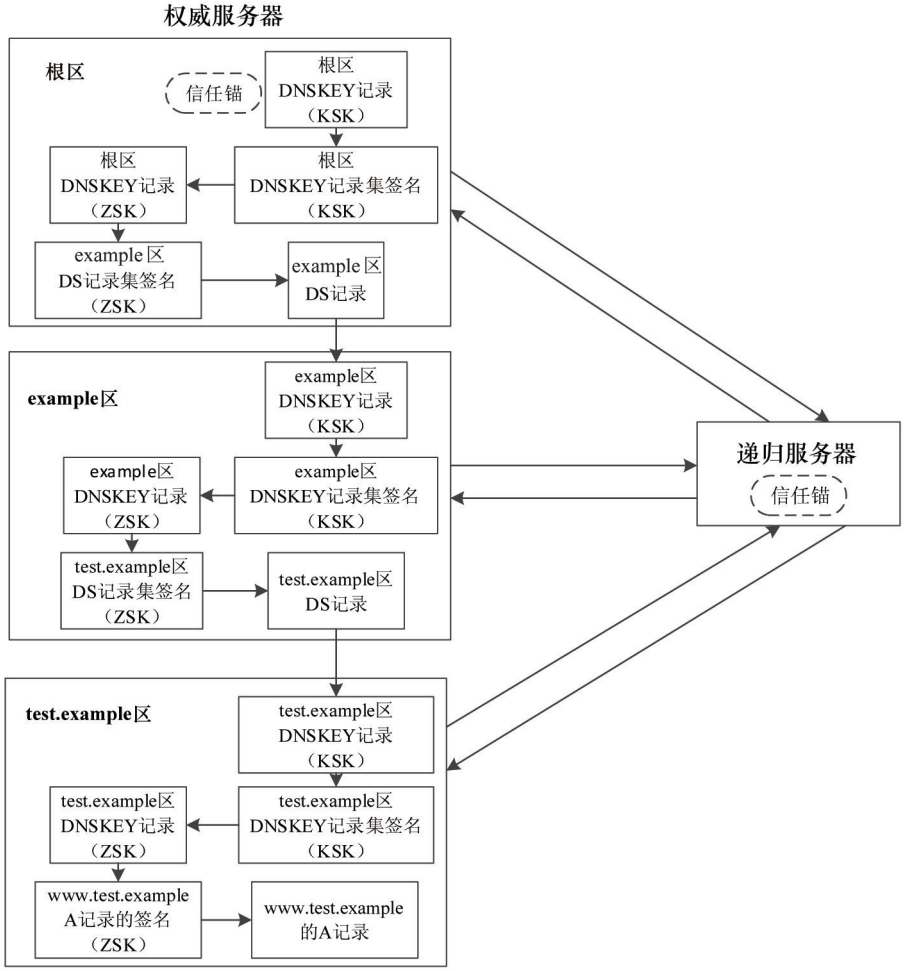

图 1　DNSSEC 信任链示意图

1.3　密钥轮转方式对比

目前 DNSSEC 密钥轮转的方式主要包括预发布轮转方式和双签轮转方式，可应用于 KSK 轮转、ZSK 轮转及算法轮转等场景。

1.3.1　预发布轮转方式

预发布轮转方式是在新密钥正式启用之前，先将其添加至 DNS 区数据中的方式，使得递归服务器在新密钥生效前能够获取新密钥。预发布轮转方式密钥生命周期如图 2 所示，权威服务器关键操作步骤如下。

（1）生成新密钥对。

（2）将新生成的密钥添加至 DNS 区数据中，作为 DNS 记录进行预发布，但尚未用于签名。

（3）进入过渡期，递归服务器获取并缓存新密钥。在此阶段，递归服务器会逐步缓存 2 组密钥。

（4）过渡期结束后，在预定时间点，完成新密钥与原密钥的正式切换，新密钥开始用于 DNS 记录的签名，同时删除原签名，原密钥无效，不再用于签名。

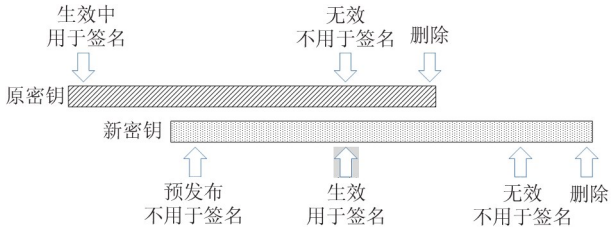

图 2　预发布轮转方式密钥的生命周期

在此阶段,递归服务器会继续使用已缓存的原密钥签名的记录,直至缓存过期失效。

(5) 新密钥处于 DNS 记录签名稳定阶段,删除原密钥,迁移结束。

1.3.2　双签轮转方式

双签轮转方式是在切换到新密钥之前,使用原密钥和新密钥同时对 DNS 记录签名的方式。这种轮转方式同时使用 2 个密钥进行签名,使得递归服务器可以验证使用原密钥签名的记录,同时支持新密钥签名记录的验证。双签轮转方式密钥生命周期如图 3 所示,权威服务器关键操作步骤如下。

(1) 生成新密钥对。

(2) 将新生成的密钥添加至 DNS 区数据中,并使用新密钥对 DNS 记录进行签名。此时 DNS 区数据中同时存在原密钥及签名,和新密钥及签名。

(3) 进入过渡期,递归服务器获取并缓存新密钥及新签名。在此阶段,递归服务器会逐步缓存 2 组密钥及签名数据。

(4) 过渡期结束后,新密钥处于 DNS 记录签名的稳定阶段。在预定时间点,删除原密钥及原签名,迁移结束。

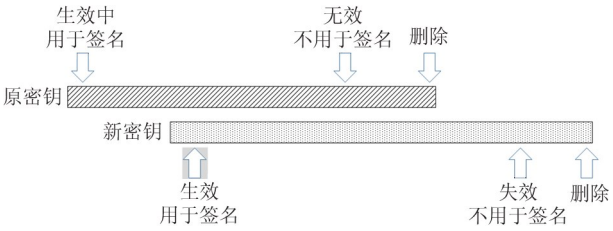

图 3　双签轮转方式密钥的生命周期

根据以上 2 种轮转方式,对其多维度特性的总结对比如表 1 所示。

表 1　预发布与双签轮转方式特性对比

特性	预发布轮转方式	双签轮转方式
迁移思路	新密钥提前发布,但未立即启用	使用新密钥和原密钥同时签名,直至过渡完成
密钥使用情况	先发布新密钥,后切换用于签名	同时使用新密钥和原密钥进行签名
过渡期	等待递归服务器缓存新密钥,过渡期长	递归服务器通过双重签名直接过渡,过渡期短
配置复杂度	需要多次操作,增加复杂性	管理 2 组签名,过渡期内需要同时维护
优点	只有一份签名数据,数据量小	快速、简洁,避免过渡期验证失败
缺点	配置较复杂,管理较麻烦	需要同时维护 2 组签名,签名数据量翻倍

1.4　顶级域 DNSSEC 密码算法应用现状

DNSSEC 涉及的密码算法包括签名算法及摘要算法。文献[14]给出了 DNSSEC 支持的签名算法,其中包括 RFC 9563 规定的 SM2SM3 签名算法(算法号 17)。截至 2025 年 4 月底,共有顶级域 1 440 余个,其中已部署 DNSSEC 的顶级域超过 1 340 个。对其进行探测及统计,当前主要使用的签名算法如表 2 所示。

如图 4 所示,超过 85% 使用 RSASHA256 算法,其次为 ECDSAP256SHA256 算法。

文献[15]给出了 DNSSEC 支持的摘要算法,其中包括 RFC 9563 规定的 SM3 摘要算法(算法号 6)。对已部署 DNSSEC 的顶级域进行探测及统计,当前主要使用的摘要算法如表3所示,其中最常用的是

表 2　顶级域使用的 DNSSEC 签名算法

算法号	算法名称
5	RSASHA1
7	RSASHA1-NSEC3-SHA1
8	RSASHA256
10	RSASHA512
13	ECDSAP256SHA256
14	ECDSAP384SHA384
15	ED25519

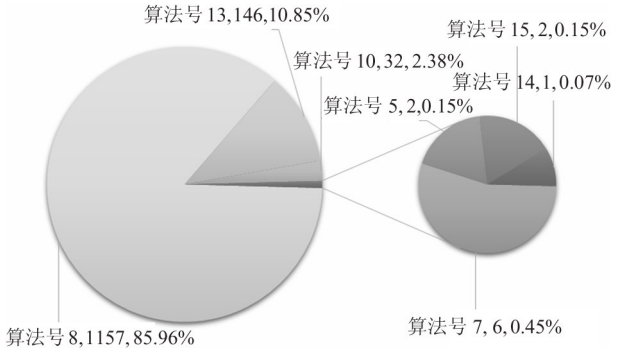

图 4 DNSSEC 签名算法应用分布

表 3 顶级域使用的 DNSSEC 摘要算法

算法号	算法名称
1	SHA-1
2	SHA-256
4	SHA-384

SHA-256 算法,使用率超过 98%。为方便选择合适的算法,文献[16]给出了强制性算法及推荐性算法的列表。

1.5 解析软件及云解析服务

为调研软件层面对 DNSSEC 的支持情况,选取了有代表性的开源解析软件及云解析服务厂商作为调研对象。

1.5.1 开源解析软件

BIND 作为全球使用最广泛的开源 DNS 解析软件,由互联网系统联盟(Internet Systems Consortium, ISC)开发维护,可提供权威和递归解析服务。NSD/Unbound 均由荷兰非盈利公益组织 NLnet Labs 开发维护。其中 NSD 是权威解析软件,Unbound 是一款轻量级高性能的递归解析软件。Knot DNS 由顶级域 CZ 的注册局 CZ. NIC 开发维护,是一款适用于高负载环境的高性能 DNS 解析软件,可提供权威和递归服务。BIND、NSD、Knot DNS 解析软件被多个根服务管理机构使用,充分证明其功能及性能方面的优势。PowerDNS 可同时提供权威和递归解析服务,支持多种后端数据库并自带管理网页,高性能、灵活性和可扩展性使其成为主流 DNS 解析软件之一。

1.5.2 云解析服务

谷歌、Cloudflare、腾讯、阿里等大型互联网公司均同时提供权威及递归云解析服务。

由多个基础电信运营商与南京信风共建的 114 DNS 也提供免费的递归服务,是国内著名的公共递归 DNS 服务。

部分大型域名注册商也提供权威云解析服务。如全球最大注册商之一的 Godaddy,同时也是国际域名解析服务商。国内著名注册商新网,是以国内市场为主的解析服务商。

2 软件及服务对 DNSSEC 的支持情况

2.1 解析软件及云解析服务对 DNSSEC 算法的支持情况

2.1.1 解析软件

开源权威解析软件对 DNSSEC 的支持情况如表 4所示。4 种软件均支持数据签名功能,并可以加载签名区数据用于对外提供解析。

开源递归软件均支持对 DNSSEC 签名进行验证的功能,如表 5 所示。

2.1.2 云解析服务

权威云解析服务对 DNSSEC 密码算法的支持情况如表6所示。6种权威云解析服务均支持DNSSEC,

表 4 权威软件对 DNSSEC 的支持情况

权威软件	BIND 9.12.1	PowerDNS 4.1.2	Knot DNS 2.6.7	NSD 4.1.22
签名区数据	支持	支持	支持	支持
加载签名区数据并提供解析	支持	支持	支持	支持
摘要算法支持情况	1/2/3/4	1/2/3/4	1/2/4	1/2/3/4
签名算法支持情况	1/2/3/5/6/7/8/10/12/13/14	5/7/8/10/12/13/14/15/16	5/7/8/10/13/14	1/2/3/4/5/6/7/8/10/12/13/14/15/16

表 5　递归软件对 DNSSEC 验签功能的支持情况

递归软件	BIND 9.12.1	PowerDNS Recursor 4.2.0	Knot DNS Resolver 4.2.0	Unbound 1.9.2
签名验证功能	支持	支持	支持	支持

表 6　权威云服务对 DNSSEC 密码算法的支持情况

权威云服务	谷歌	Cloudflare	腾讯	阿里	Godaddy	新网
摘要算法支持情况	1/2/4	1/2/3/4	1/2/3/4	1/2/3/4	1/2/3/4	1/2/3/4
签名算法支持情况	8/10/13/14	8/10/13/14	5/7/8/10/12/13/14	1/2/3/5/6/7/8/10/12/13/14/15/16/252/253/254	5/7/8/10/12/13/14	5/7/8/10/12/13/14

对 RSASHA256(算法号 8)、RSASHA512(算法号 10)、ECDSAP256SHA256(算法号 13)、ECDSAP384SHA384(算法号 14)4 种算法的支持情况较好。

公共递归服务对 DNSSEC 签名验证功能的支持情况如表 7 所示。部分公共递归服务不支持 DNSSEC 签名验证功能。

表 7　公共递归服务对 DNSSEC 签名验证功能的支持情况

公共递归服务	服务地址	支持签名验证功能
谷歌	8.8.8.8 8.8.8.4	是
Cloudflare	1.1.1.1	是
腾讯	119.29.29.29	否
阿里	223.5.5.5 223.6.6.6	否
114DNS	114.114.114.114	否

2.2　安全软件库对 SM 系列算法的支持情况

根据文献[17]所述,主流安全软件库中 OpenSSL、GmSSL、铜锁/Tongsuo 项目对国密算法支持较好,均支持 SM2 及 SM3 算法,适合作为 DNSSEC 扩展支持 SM2SM3 算法的第三方软件库。

2.2.1　OpenSSL

OpenSSL 是一个开源软件库和命令行工具,用于实现安全通信的 SSL(secure socket layer)和 TLS(transport layer security)协议。OpenSSL 可用于生成密钥和证书、加密数据和验证证书,已成为互联网安全和服务器管理的必备工具。OpenSSL 1.1.1[18]及更高版本支持算法 SM2、SM3 和 SM4。

2.2.2　GmSSL

GmSSL 是一个开源的密码工具箱,GmSSL 项目[19]由北京大学开发维护,支持 SM2/SM3/SM4/SM9 等国家商用密码算法,支持国密硬件密码设备。GmSSL 项目是 OpenSSL 项目的分支,并与 OpenSSL 保持接口兼容。因此 GmSSL 可以替代应用中的 OpenSSL 组件,并使应用自动具备基于国密的安全能力。

2.2.3　铜锁/Tongsuo

铜锁[20]/Tongsuo(原 BabaSSL)是一个提供现代密码学算法和安全通信协议的开源基础密码库,是由开放原子开源基金会(OpenAtom Foundation)孵化的开源项目。可实现数据在传输、使用、存储等过程中的私密性、完整性和可认证性,为数据生命周期中的隐私和安全提供保护能力。铜锁/Tongsuo 项目支持 SM2、SM3 和 SM4 等算法,也是 OpenSSL 分支之一。

2.3　软件层面实现 DNSSEC 支持 SM2SM3 算法的解决方案

2.3.1　推动安全软件库对 SM 系列算法的支持

SM 系列算法作为我国自主设计的密码标准,虽然已经成为国际标准,但其在安全软件库的底层集成及广泛适配尚未实现。为推动安全软件库对 SM 系列算法的支持,可以从主流软件库和已支持 SM 系列算法的软件库 2 个维度协同发力。一方面是深化主流安全软件库的原生支持,着力推动

OpenSSL 等国际主流密码学工具对 SM 系列算法的原生集成,降低开发者的使用门槛;另一方面是优化国产密码库的国际互认,在持续完善 GmSSL、铜锁/Tongsuo 等成熟国产密码库的同时,提升其在密码行业内的使用率,积极参与 NIST 密码算法验证计划(cryptographic algorithm validation program,CAVP)等国际权威互操作性测试,全面提升 SM 系列算法的国际认可度。

2.3.2　推动解析软件及服务对 SM 系列算法的支持

解析软件及服务的改造工作分为 2 个阶段。第 1 阶段面向权威域名解析软件,在 BIND、Knot DNS、PowerDNS 等主流开源权威域名解析软件中实现对 DNSSEC 中 SM2SM3 签名算法及 SM3 摘要算法的集成适配,在数据签名环节搭建应用 SM 商用密码算法的基础。第 2 阶段面向递归解析服务,完成运营商递归服务与公共递归服务的国密兼容改造,在数据校验环节补齐对 SM 商用密码算法的支撑。递归解析服务作为连接权威解析服务与终端用户的核心中转节点,完成该环节的算法适配改造,是实现 DNSSEC 域名解析全流程兼容 SM 商用密码算法的关键步骤。

3　签名算法迁移方案

3.1　签名算法迁移的目标与关键问题

对于首次部署 DNSSEC 的域名,可直接使用 SM2SM3 算法的密钥对 DNS 数据签名。此种情况操作步骤简单,过程中不涉及签名算法的变更,容易保证信任链完整可验证。但对于已部署 DNSSEC 的域名,如果替换其所使用的签名算法,操作相对复杂,在变更过程中信任链会发生变化,需要充分考虑各步操作信任链的完整性和可验证性。本节讨论的签名算法迁移的对象是已部署 DNSSEC 的域名,目标是从当前使用的签名算法平滑过渡至 SM2SM3 算法。

签名算法迁移过程中,通过密钥轮转的方式将 DS 记录、DNSKEY 记录、RRSIG 记录替换为使用 SM2SM3 算法的对应记录。为实现平滑过渡,其关键问题是保证迁移期间域名信任链不中断,并确保签名的正确性、有效性,从而保证业务的连续性。

3.2　算法迁移操作步骤

综合考虑签名数据量及操作复杂度,KSK 通常采用双签轮转方式,ZSK 通常采用预发布轮转方式。文献[21]给出了 KSK 双签轮转和 ZSK 预发布轮转的实例。

本文中算法迁移同时涉及 KSK 及 ZSK 轮转,根据 RFC 6781 建议,均采用双签轮转方式。算法迁移过程中,父区及子区先后出现的所有区数据示意可参见图 5,迁移阶段可参见图 6,其中子区为迁移的目标域名。算法迁移的核心目标是更换密钥及签名,因此 DNSKEY 记录及 RRSIG 记录会发生变化,进一步地,该操作会引起 DS 记录的变化。每个阶段的操作及区数据内容的变化说明如下。

(1) 初始状态:算法迁移前,父区中的 DS 记录、子区中的 DNSKEY 记录和 RRSIG 记录均使用原算法。

(2) 添加新 RRSIG 记录:子区增加国密密钥生成的 RRSIG 记录,但不添加国密密钥本身。此阶段,使用国密密钥签名的 RRSIG 记录将被更新至递归服务器的缓存中。

(3) 添加新 DNSKEY 记录:在原签名数据在缓存中过期后,将国密密钥添加至 DNS 区数据中。此阶段需要等待新 RRSIG 记录被缓存后,方可开始。

(4) 变更 DS 记录:在国密 DNSKEY 记录缓存生效后,将国密DNSKEY记录(KSK)的DS记录更

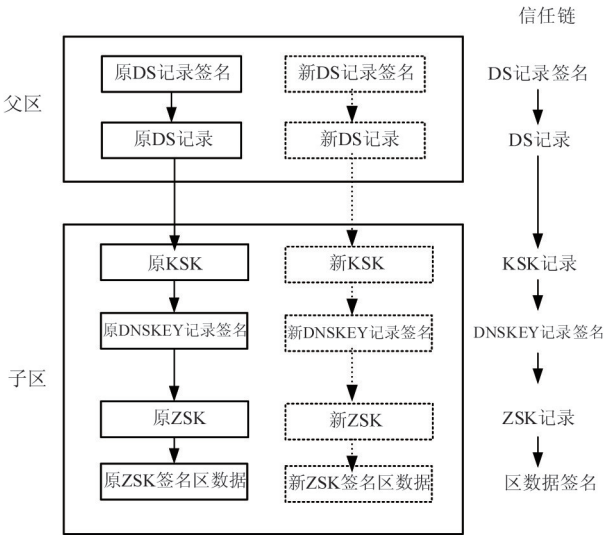

图 5　DNSSEC 算法迁移区数据示意图

新到父区,并删除原 DNSKEY 记录(KSK)的 DS 记录。此阶段需要等待新 DNSKEY 记录被缓存后,方可开始。

(5) 删除原 DNSKEY 记录:原密钥退出解析系统,删除原 DNSKEY 记录。此阶段需要等待新 DS 记录被缓存后,方可开始。

(6) 删除原 RRSIG 记录:原签名退出解析系统,删除原 RRSIG 记录。

3.3 算法迁移过程中的 DNSSEC 信任链分析

如图 5 所示,信任链的验证包括父区的 DS 记录、子区的 KSK 记录、子区 DNSKEY(含 ZSK 及 KSK)的 RRSIG 记录、子区的 ZSK 记录及子区 DNS 记录的 RRSIG 记录。在算法迁移过程中,先由子区同时加载新旧算法的 RRSIG 记录,再添加使用新算法的新 DNSKEY(含 ZSK 及 KSK)记录,此时子区存在 2 条 DNSSEC 信任链。然后通过父区 DS 记录的更换,废除旧算法,迁移为新算法。迁移过程中每个阶段信任链可验证情况如表 8 所示,可见在迁移过程中始终存在可验证通过的完整信任链,因此可以保证业务的连续性。

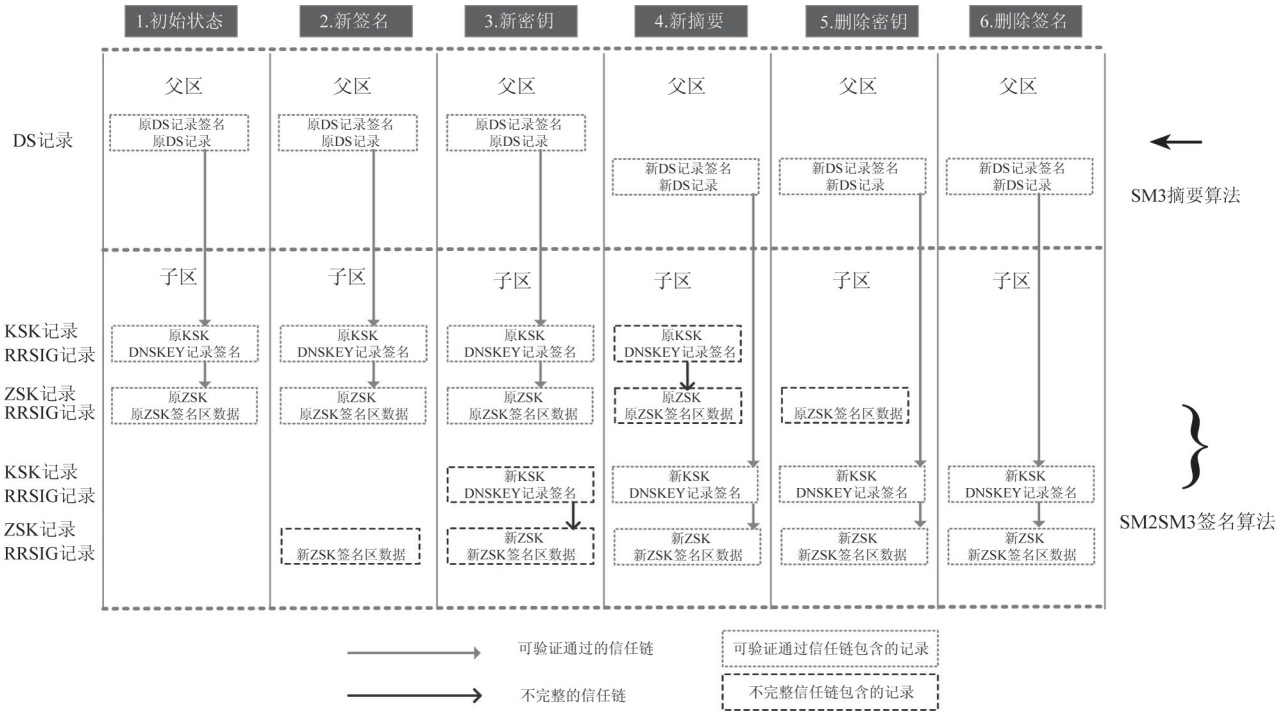

图 6 DNSSEC 算法迁移阶段

表 8 迁移各阶段 DNSSEC 信任链情况

序号	阶段	父区中 DS 记录	子区中 DNSKEY 记录	子区中 RRSIG 记录	信任链是否可验证通过	数据是否可验证
1	初始状态	原 KSK DS 记录	原 KSK/ZSK 记录(使用原 KSK 签名)	区数据的 RRSIG 记录(使用原 ZSK 签名)	是	是
2	添加新 RRSIG 记录	原 KSK DS 记录	原 KSK/ZSK 记录(使用原 KSK 签名)	区数据的 RRSIG 记录(使用原 ZSK 签名)	是	是
		缺失	缺失	区数据的 RRSIG 记录(使用新 ZSK 签名)	否	
3	添加新 DNSKEY 记录	原 KSK DS 记录	新旧 KSK/ZSK 记录(使用原 KSK 签名)	区数据的 RRSIG 记录(使用原 ZSK 签名)	是	是
		缺失	新旧 KSK/ZSK 记录(使用新 KSK 签名)	区数据的 RRSIG 记录(使用新 ZSK 签名)	否	

（续表 8）

4	变更 DS 记录	缺失	新旧 KSK/ZSK 记录（使用原 KSK 签名）	区数据的 RRSIG 记录（使用原 ZSK 签名）	否	是
		新 KSK DS 记录	新旧 KSK/ZSK 记录（使用新 KSK 签名）	区数据的 RRSIG 记录（使用新 ZSK 签名）	是	
5	删除原 DNSKEY 记录	缺失	缺失	区数据的 RRSIG 记录（使用原 ZSK 签名）	否	是
		新 KSK DS 记录	新 KSK/ZSK 记录（使用新 KSK 签名）	区数据的 RRSIG 记录（使用新 ZSK 签名）	是	
6	删除原 RRSIG 记录	新 KSK DS 记录	新 KSK/ZSK 记录（使用新 KSK 签名）	区数据的 RRSIG 记录（使用新 ZSK 签名）	是	是

4　实验验证

4.1　实验环境及方法

为验证第 3 节所述迁移方案，搭建实验环境如图 7 所示，包括根区服务器、example 区服务器和模拟递归服务器。根区服务器和 example 区服务器使用 ISC BIND 解析软件，版本为 9.10.3-P4，分别加载根区数据和 example 区数据并提供解析服务。模拟递归服务器使用基于 dnspython 2.2.1 编写的模拟程序，实现递归服务器的查询、缓存及验证功能。

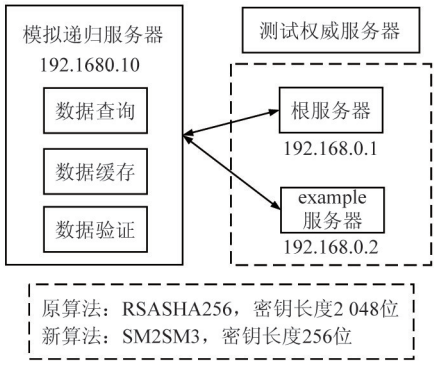

图 7　实验环境及数据

为便于对比分析，选择目前主流的 RSASHA256 作为迁移前算法，迁移后使用 SM2SM3 算法。实验数据中 DNSKEY 记录的说明如表 9 所示。

根区数据包括根区的 DNSKEY 记录及 example 区的 DS 记录。初始状态时，DS 记录为使用 SHA256 算法生成的摘要，摘要原始数据是 Key Tag 为 9 352 并使用 RSASHA256 算法签名的 DNSKEY 记录。迁移结束后，DS 记录为使用 SM3 算法生成的摘要，摘要原始数据是 Key Tag 为 27 215 并使用 SM2SM3 算法签名的 DNSKEY 记录。根区数据中，example 区的 DS 记录如图 8 所示。

表 9　实验数据中 DNSKEY 记录说明

序号	Key Tag	DNSKEY 用途说明	算法	密钥长度/bit
1	9 352	原 KSK 密钥	RSASHA256（算法号 8）	2 048
2	48 315	原 ZSK 密钥	RSASHA256（算法号 8）	2 048
3	27 215	新 KSK 密钥	SM2SM3（算法号 17）	256
4	65 042	新 ZSK 密钥	SM2SM3（算法号 17）	256

```
. IN DNSKEY 257 3 8 公钥省略 ——信任锚
example. IN DS 9352 8 2
  6485B08BA1991CD7D8FAF6F790E3 82866588FA8470E27222500E9168
  BBCEF9B8 ——初始状态
example. IN DS 27215 17 6
  BBF66976530DB9E6AD80C843D3DC 03C815CD1934AA9065CBFC620396
  87EB9A20 ——结束状态
```

图 8　根区中的 DS 记录

example 区数据包括 example 区的 DNSKEY 记录、A 记录及 RRSIG 记录。初始状态时，RRSIG 记录为使用 RSASHA256 算法生成的签名，签名原始数据是 A 记录，签名使用的私钥是 Key Tag 为48 315的 DNSKEY 记录对应的私钥。迁移结束后，RRSIG 记录为使用 SM2SM3 算法生成的签名，签名原始数据不变，签名使用的私钥是 Key Tag 为65 042的 DNSKEY 记录对应的私钥。example 区 RRSIG 记录如图 9所示。

模拟递归服务器将根区公钥设置为信任锚，依次查询根区服务器及 example 区服务器，将权威服务器响应数据放入缓存，并依据缓存数据对信任链

```
test.example. 3600    IN A         10.10.1.1
test.example. 3600    IN RRSIG A 8 2 3600 (
     20250601000000 20250401000000 48315 example.
wh9RjTXTKfS0O2XgN4qW4Q7Oshw2UjUc/5gg3TViHpEHk0PveBUs7xwv
Kxkd1PEQT6xgXUyZpbA2b39M6YWX3WoR251e2oaVrnSxthog2nSuf5I7
A0NAyPIZALaPjcZtMqxSdQAsI+cSc znkXlXp/4DicQlqON90DZpqI0WH
RZzs/8KfOYgowGsAkAjpZVM6i4nPN9lV49t7LXMVWdR7W8mVBXenGLgF
BjzqY6sV6u7TuPEqSGMHPEnZiCAjbyVQM/7kLzEQ2yFNuWv6dx0iVyd5
eQWaOtN1/Zrl1daU7lrazY/saGG6RkPkg+H5dM3miT8V09MgIDp/FDRw
MQQEvw==)                              ——初始状态
test.example. 3600    IN RRSIG A 17 2 3600 (
     20250606000000 20250406000000 65042 example.
5T4k0SzbQxbgLIH8I/Q+hOnd2Fe3R8kjzMKxp0gfII31v2DGNrxZUJbq
PH51IOItIBxgmbEOc+678IahHTDoyw==) ——结束状态
```

图 9　example 区中的 RRSIG 记录

各记录进行验证。若验证通过,则响应数据包中 AD(Authenticated Data)标志位置 1。

4.2　实验结果及分析

4.2.1　信任链验证结果

实验结果表明,迁移各阶段均可对 test.example 的 A 记录进行验证,验证通过的信任链所包含的 DS 记录、DNSKEY 记录、RRSIG 记录如表 10 所示。由阶段 4 开始,验证通过的信任链变更为使用新算法的记录。

表 10　迁移各阶段可验证信任链

序号	阶段	根区中 DS 记录	Example 区中 DNSKEY 记录	Example 区中 RRSIG 记录	响应数据包 AD 标志位
1	初始状态	Key 9352 的摘要	KSK 记录(9352) ZSK 记录(48315)	Key 9352 生成的签名 Key 48315 生成的签名	1
2	添加新 RRSIG 记录	Key 9352 的摘要	KSK 记录(9352) ZSK 记录(48315)	Key 9352 生成的签名 Key 48315 生成的签名	1
3	添加新 DNSKEY 记录	Key 9352 的摘要	KSK 记录(9352) ZSK 记录(48315)	Key 9352 生成的签名 Key 48315 生成的签名	1
4	变更 DS 记录	Key 27215 的摘要	KSK 记录(27215) ZSK 记录(65042)	Key 27215 生成的签名 Key 65042 生成的签名	1
5	删除原 DNSKEY 记录	Key 27215 的摘要	KSK 记录(27215) ZSK 记录(65042)	Key 27215 生成的签名 Key 65042 生成的签名	1
6	删除原 RRSIG 记录	Key 27215 的摘要	KSK 记录(27215) ZSK 记录(65042)	Key 27215 生成的签名 Key 65042 生成的签名	1

4.2.2　RSASHA 算法与 SM2SM3 算法签名大小分析

如图 9 所示,RSASHA 算法(密钥长度 2 048 bit)生成的签名长度为 256 字节(Byte,B),而 SM2SM3 算法生成的签名长度为 64 B。4.1 实验中需传输 3 条 RRSIG 记录,实际查询过程中还可能涉及多个权威服务器的查询,使用不同签名算法的数据包大小总差异将更为显著。

通过对 2 种算法签名数据大小的对比可见,使用 SM2SM3 算法可有效减少网络传输数据量,一方面可以缩短数据传输的耗时,提升递归服务器获取数据验证签名过程的效率;另一方面,更为重要的是,较小的响应数据可以有效防止 DNSSEC 被用作 DDoS 攻击手段。

5　结　论

本文从软件实现和运维部署的角度,对 DNSSEC 支持 SM2SM3 算法的关键问题进行了研究,并归纳总结出多个有价值的结论。首先,对行业主流 DNS 软件及服务提供商对 DNSSEC 算法的支持现状进行了调研归纳,发现主流开源权威、递归解析软件及权威云解析服务对 DNSSEC 的支持程度较好,部分公共递归服务不支持 DNSSEC。为实现 DNSSEC 对 SM2SM3 算法的支持,关键在于安全软件库对 SM 系列算法的支持程度,通过向主流安全软件库贡献代码或推广已全面支持 SM 系列算法的安全软件库,可有效提升软件及服务的支持程度。尤其是递归服务,作为连接权威解析服务和客户端的桥梁,在推动解析服务支持 SM2SM3 算法过程中的角色至关重要。接下来,本文根据 RFC 6781 形成完整的算法迁移方案,并对算法迁移方案的可行性进行了理论论证及实验验证,确保在算法迁移过程中的业务连续性。本文所述方法适用于任意 2 种密码算法间的迁移。在实际部署过程中,还需要充分考虑到递归解析服务支持 SM2SM3 算法的进展会相当

缓慢。根据以往经验,该过程可能在 5 年以上,因此需保证足够长的算法并行期,采用 SM2SM3 算法的同时,还需采用一种强制性的 DNSSEC 算法,避免出现递归无法验证 SM2SM3 算法导致的信任链断裂问题而影响解析数据可用性。

参考文献

[1] Arends R, Austein R, Larson M, et al. DNS security introduction and requirements: RFC 4033[S]. San Diego: Internet Engineering Task Force, 2005.

[2] Arends R, Austein R, Larson M, et al. Resource records for the DNS security extensions: RFC 4034[S]. San Diego: Internet Engineering Task Force, 2005.

[3] Arends R, Austein R, Larson M, et al. Protocol modifications for the DNS security extensions: RFC 4035[S]. San Diego: Internet Engineering Task Force, 2005

[4] 苏彬庭, 陈明志, 许力, 等. 国密算法在工业互联网安全中的应用研究[J]. 信息技术与网络安全, 2021, 40(3):28 - 31.

[5] 赵晗, 王燕娜, 李建峰. 国产密码在城市轨道交通综合监控系统中的应用[J]. 城市轨道交通研究, 2021, 24(5):171 - 174,178.

[6] 黄恺彤, 刘晔. 国产密码算法在电网信息安全中的应用研究[J]. 信息安全与通信保密,2015(10):82 - 83.

[7] 冷峰, 张明凯, 延志伟, 等. 国密算法在资源公钥基础设施(RPKI)中的应用[J]. 计算机科学, 2021, 48(Z2):678 - 681.

[8] 侯宪锋,韩磊,王兴元,等. 国密算法在智能家居数据安全应用研究[J]. 中国新通信,2021,23(20):49 - 51.

[9] 胡景秀, 杨阳, 熊璐, 等. 国密算法分析与软件性能研究[J]. 信息网络安全, 2021(10):8 - 16.

[10] Barker E, Barker W, Burr W, et al. Recommendation for key management part 1: general (revision 3): NIST SP 800-57[R]. San Diego: National Institute of Standards and Technology, 2012.

[11] Müller M,Toorop W,Chung T,et al. The reality of algorithm agility: studying the DNSSEC algorithm life-cycle[C]// Proceedings of the ACM Internet Measurement Conference. Online: ACM, 2020:295 - 308.

[12] Kolkman O, Mekking W, Gieben R. DNSSEC operational practices, version 2: RFC 6781[S]. San Diego: Internet Engineering Task Force, 2012.

[13] Schomp K, Callahan T, Rabinovich M, et al. On measuring the client-side DNS infrastructure[C]// Internet Measurement Conference. Barcelona, Spain: ACM, 2013: 77 - 90.

[14] IANA. DNSSEC delegation signer(DS) resource record(RR) type digest algorithms[EB/OL]. (2024 - 12 - 05)[2025 - 04 - 30]. https://www.iana.org/assignments/ds-rr-types/ds-rr-types.xhtml.

[15] IANA. Domain name system security (DNSSEC) algorithm numbers[EB/OL]. (2024 - 12 - 05)[2025 - 04 - 30]. https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml.

[16] Wouters P, Sury O. Algorithm implementation requirements and usage guidance for DNSSEC: RFC 8624[S]. San Diego: Internet Engineering Task Force, 2019.

[17] 方方明,袁志昌,曹佩庆,等. 商用密码技术最佳实践白皮书[EB/OL]. (2023 - 03 - 24)[2025 - 05 - 12]. https://openanolis.github.io/whitebook-shangmi/openanolis.html.

[18] OpenSSL. OpenSSL documentation[EB/OL]. (2018 - 09 - 11)[2025 - 04 - 30]. https://docs.openssl.org/1.1.1.

[19] GmSSL. GmSSL 项目官网[EB/OL]. (2014 - 12 - 31)[2025 - 04 - 30]. http://gmssl.org.

[20] 铜锁/Tongsuo. 铜锁/Tongsuo 项目官网[EB/OL]. (2022 - 12 - 12)[2025 - 04 - 30]. https://tongsuo.net.

[21] 何峥, 冷峰, 张翠玲. 在 DNSSEC 下保障顶级域名解析托管服务稳定迁移的操作机制[J]. 网络与信息安全学报, 2021,7(3):156 - 165.

Research and application on DNS security extentions based on SM2SM3 algorithm

Zhang Cuiling, Sun Qi, He Zheng, Tang Hongfeng, Jiang Yufeng, Li Shuailiang, Li Hanming

(China Internet Network Information Center, Beijing 100070)

Abstract

As the infrastructure of the Internet, the domain name system (DNS) is responsible for translating human-readable domain names into machine-readable Internet procotol (IP) addresses. However, traditional DNS protocols did not adequately consider security in their design and are susceptible to security threats such as cache poisoning and man-in-the-middle attacks. DNS security extensions (DNSSEC) ensures the integrity and authenticity of DNS responses by introducing a digital signature mechanism, which can effectively enhance DNS security to avoid these attacks. DNSSEC supports multiple cryptographic algorithms, and RFC 9563 specifies the format of DNS public key (DNSKEY) and resource record signature (RRSIG) resource records, and the algorithm number for using the SM2SM3 algorithm in DNSSEC. To promote the application of Shangmi algorithms in the field of DNSSEC, this paper analyzes and investigates the key challenges from both software and operational perspectives, and proposes solutions for DNSSEC implementation based on SM2SM3 algorithm.

Key words: domain name system (DNS), DNS security extensions, DNS security extentions algorithm rollover, SM cryptography algorithms