根区 KSK 轮转计划

设计团队报告草案 - 更新日期：2015 年 8 月 4 日

1 概述

ICANN 正在准备有关进行根区 DNSSEC 密钥签名密钥 (KSK) 轮转的计划。ICANN 正在以其 IANA 职能运营商的身份，与其他根区管理 (RZM) 合作伙伴一起计划这项轮转工作。这些合作伙伴包括威瑞信（Verisign，作为根区维护机构）和美国国家电信和信息管理局（NTIA，作为根区管理机构）。[1]

轮转根区 KSK 指的是更改自 2010 年起一直在使用的密钥，当时是根据域名系统安全扩展 (DNSSEC) 的定义首次对根区进行签名[2]。更改密钥意味着会生成新的加密密钥组件，并且会分发新的公共组件。充分分发新的公共组件是密钥轮转工作的最关键方面。

本文档是设计团队协商结果的报告草案，接受公众意见，设计团队由所招募的 DNS 和 DNSSEC 专家志愿者小组，以及根区管理合作伙伴组成。本文档为草案，将根据在 ICANN 的公开公共评议期内所获得的互联网社群意见和建议，以及进一步的协商结果来加以修订。在经过后续讨论之后，将发布最终报告。

2 目录

[1] 这份计划草案是按照 IANA 职能合同，以及 NTIA 与威瑞信之间的合作协议中所指定的最新根区管理结构而制定。设计团队与根区管理合作伙伴承认当前正在进行的 IANA 管理权移交工作可能会对 KSK 轮转计划，以及 NTIA 参与任何未来工作流程产生影响。但是，技术细节和注意事项在很大程度上与移交工作及其最终结果无关。

[2] 请参阅 RFC 4033、RFC 4034 和 RFC 4035

3 执行摘要

ICANN 作为 IANA 职能运营商，通过与作为根区维护机构的威瑞信和作为根区管理机构的美国国家电信和信息管理局 (NTIA) 进行协作，一直致力于制定有关轮转根区密钥签名密钥 (KSK) 计划。ICANN、威瑞信和 NTIA 组成了根区管理 (RZM) 合作伙伴。

根据 DNSSEC，根区 KSK 用于对根区 DNSKEY 资源记录集进行签名。此集合包括域签名密钥 (ZSK)，用于对根区内的所有其他资源记录集 (RRset) 进行签名。轮转根区 KSK 是指更改自 2010 年起一直使用至今的密钥（当时根区是根据 DNSSEC 首次签名的）。更改密钥意味着会生成新的加密密钥组件，并且会分发新的公共组件。充分分发新的公共组件是密钥轮转工作的最关键方面。

2014 年 12 月，ICANN 请求社群志愿者与 RZM 合作伙伴一起参加设计团队，以制定本文档中所展示的根区 KSK 轮转计划。此项工作要获得的成果是一组全面的技术和运作建议，用于指导 RZM 合作伙伴制定出有关执行首次根区 KSK 轮转的详细实施计划。应将本文档视作提供这些可交付成果的计划草案。

3.1 DNS 术语

本文档介绍关于 DNS 和 DNSSEC 的技术详细信息。由于已有 DNSSEC 相关术语的定义，下面的 **Error! Reference source not found.**中提供了一些相关术语定义。

术语	简写	说明
资源记录集	RRSet	存储在 DNS 内的数据单元，是由 DNSSEC 密钥签名的最小单位
密钥签名密钥	KSK	公钥-私钥对[3]，其角色是生成 DNS 域中使用的密钥集的可验证签名。此角色很特殊，因为 DNSSEC 要求将此类公钥在 DNS 协议之外进行发布
域签名密钥	ZSK	一个公钥-私钥对，其角色是生成 DNS 域中所有其他数据集的签名。此密钥在 DNS 协议之外分发

[3] Niels Ferguson；Bruce Schneier (2003)。《*Practical Cryptography*》（加密技术实战）。Wiley。ISBN 0-471-22357-3。

术语	简写	说明
DNSKEY RRset		域中使用的密钥集，包括 KSK 和 ZSK 的角色，是一组 DNSKEY 资源记录
密钥轮转		按一定顺序从一种加密密钥改为另一种加密密钥的行为
(DNSSEC) 验证程序		对 DNSSEC 响应执行安全检查（包括验证数据签名的步骤）的软件
信任锚		验证程序绝对信任的已存储公共 KSK
自动更新 DNSSEC 信任锚	RFC 5011	在验证程序中自动更新信任锚的一种方法
双签名		包含 RRset 的两个签名，通常在轮转中使用新旧密钥。通常一个签名就足够 RRset 使用了
根服务器系统咨询委员会	RSSAC	在 ICANN 章程中已经规定，职能是向 ICANN 社群提供有关根服务器系统的建议
DNS 扩展机制	EDNS 或 EDNS(0)	当前在 RFC 6891 中定义，目的是提供一种扩展原始 DNS 协议格式的方法。EDNS(0) 指的是第一组扩展
授权签署人资源记录	DS	表示转授权中使用的 KSK 的 DNSSEC 记录（对于根区则表示顶级域的 KSK）
否定答案	NSEC 或 NSEC3	DNSSEC 定义的资源记录，用于指示对于所提问题不存在任何数据
DNSSEC 实践准则	DPS	描述针对域的 DNSSEC 具体处理方式的文档。
密钥签名仪式		在硬件安全模块内使用私钥生成签名的事件。证人需要查看管理时使用的正式流程。

表 1.DNS 和 DNSSEC 术语

3.2 其他安全术语

术语	简写	说明
OpenPGP	OpenPGP	一种管理公钥-私钥的方法。RFC 4880:*OpenPGP 消息格式*
加密消息语法标准	PKCS#7	RFC 2315:*PKCS #7：加密消息语法 - V1.5*
目录 - 公钥和属性证书框架	X.509	管理公钥-私钥的国际电信联盟电信标准部门 (ITU-T) 标准。ITU-T 建议 X.509 | ISO/IEC 9594-8
密钥签名请求	KSR	一个数据结构，其中包含对密钥进行签名的请求，尤其是需要 KSK 签名的 DNSKEY 集
签名密钥响应	SKR	一个数据结构，其中包含私钥生成的签名，尤其是针对 DNSKEY 集的 KSK 签名

表 2.其他安全术语

3.3 其他网络术语

其他一些所使用的可能需要为普通受众定义的术语

术语	简写	说明
用户数据报协议	UDP	用于在互联网上发送数据的无上下文的、最有效的传输协议
传输控制协议	TCP	用于在互联网上发送数据的面向连接的、按八位字节顺序提供保证的传输协议
最大传输单元	MTU	在部分互联网上发送的数据中可包含的最大八位字节数，“路径最大传输单元”是指互联网端到端行程中使用的所有部分的最小 MTU

表 3.其他网络术语

3.4 建议摘要

建议 1：根区 KSK 轮转应遵循 RFC 5011 中描述的过程，在 KSK 轮转期间更新信任锚。

建议 2：ICANN 应确定关键 DNS 软件供应商，并与之密切协作，以制定出正式流程，确保使用特定于供应商的渠道分发信任锚是健全且安全的。

建议 3：ICANN 应确定关键 DNS 系统集成商，并与之密切协作，以制定出正式流程，确保使用特定于集成商的渠道分发信任锚是健全且安全的。

建议 4：ICANN 应积极推广适当的根区信任锚身份验证，包括强调在 ICANN 的 IANA 网站上发布的信息。

建议 5：根区 KSK 轮转不应对现有 KSK 管理和使用流程进行任何实质性更改，以保持与之相关的高透明度标准。

建议 6：对根区 DNSKEY RRset 的所有更改都必须符合 KSK 运营商的 DPS 中所描述的 10 天的时间段。

建议 7：应保留第一次根区 KSK 轮转的新 KSK 的现有算法和密钥大小。

建议 8：对于以后的根区 KSK 轮转，应审核所选择的算法和密钥大小。

建议 9：ICANN 应与 RZM 合作伙伴协作设计并执行沟通计划，以提高对根区 KSK 轮转的认知，包括通过适当的技术性会议与全球技术性社群进行外展活动，以及与“渠道合作伙伴”（例如，本文中指出的那些合作伙伴）进行外展活动。

建议 10：ICANN 应在 KSK 轮转期间的详细时间表发布之前，要求 RSSAC 协调开展一次对这份时间表的审核，并且应提出合理的请求，以在任何根服务器运营商确定由于运作方面的原因需要修改此时间表时，对此时间表进行相应的修改。

建议 11：ICANN 应与 RSSAC 和 RZM 合作伙伴进行协调，以确保使用实时沟通渠道来保证根服务器系统能够很好地感知根区内每一次涉及添加或移除 KSK 的变化。

建议 12：ICANN 应与 RSSAC 进行协调，请求根服务器运营商执行数据收集以协助后续分析，并帮助明确 KSK 轮转对运行的影响，并让第三方分析能够使用数据收集计划和结果。

建议 13：RZM 合作伙伴应确保将来增加 ZSK 大小时都要仔细考虑 KSK 轮转，以避免同时开展这两项工作。

建议 14：为最大限度地缩短因涉及新 KSK 的困难所造成的恢复时间，在新 KSK 生成 SKR 的同时，当前 KSK 也应生成 SKR。

建议 15：RZM 合作伙伴应制定并记录必须使用当前 KSK 生成的 SKR 的流程。

3.5 受众

本文档面向技术受众，尤其是熟悉 DNS 和 DNSSEC 协议、DNS 运营方面，以及与在根区内使用 DNSSEC 相关流程的受众。

3.6 文档内容范围

本文档旨在建立框架并提供一组建议，以指导 RZM 合作伙伴制定出根区 KSK 轮转的详细实施计划。

4 简要历史回顾

4.1 在根区内部署 DNSSEC

2009 年，RZM 合作伙伴通过协作[4]在根区部署了 DNSSEC，并最终于 2010 年 7 月首次发布了可验证的已签名根区。当前使用的根区 KSK 是在首次 KSK 仪式中生成的，这次仪式在位于美国弗吉尼亚州库尔佩珀的安全密钥管理设施 (KMF) 内召开，该设施由 ICANN 管理。密钥资料后续被转移至美国加利福尼亚州埃尔塞贡多举办的第二次 ICANN KMF，KSK 的公用部分在经证实已安全完成转移之后，即在根区内作为信任锚发布了。

NTIA 要求生成和维护根区 KSK，以及每个 RZM 合作伙伴各自的职责[5]。在单独的 DNSSEC 策略和实践准则 (DPS) 中发布了根区维护机构和 IANA 职能运营商满足这些要求需遵循的过程[6]。

NTIA 与 ICANN 之间的 IANA 职能合同于 2010 年 7 月经过修改，在其中包含了与根区 KSK 管理相关的职责，在此合同的后续修订版中推进了这些要求[7]。NTIA 与威瑞信之间的合作协议也在 2010 年 7 月进行了修改，以反映威瑞信所承担的根区 ZSK 运营商职责。[8]

[4] 在以下网址发布了有关在根区内部署 DNSSEC 的详细信息：http://www.root-dnssec.org/
[5] 《在权威根区初次部署 DNSSEC 的测试和执行要求》，2009 年 10 月 29 日：http://www.ntia.doc.gov/files/ntia/publications/dnssec_requirements_102909.pdf
[6] https://www.iana.org/dnssec，https://www.verisigninc.com/en_US/repository/index.xhtml

[7] http://www.ntia.doc.gov/page/iana-functions-purchase-order
[8] http://www.ntia.doc.gov/files/ntia/publications/amendment31_07062010.pdf

IANA 职能合同要求 ICANN 执行根区 KSK 轮转，但未指定详细的时间表或实施计划。根区 KSK 运营商 DPS 中包含此声明，在第 6.5 节中提出了有关轮转的要求：

“每个 RZ KSK 都将安排通过所要求的密钥仪式进行轮转，或在运营 5 年后进行更新。”

4.2 有关根区 KSK 轮转计划的公众意见

2013 年 3 月 8 日，ICANN 开放了公共评议期，以期获得有关执行根区 KSK 轮转计划的反馈[9]。共计有六家机构和 15 名个人给予了回应。ICANN 通过对收到的回应进行总结[10]，确定了供 RZM 合作伙伴考量的七项建议：

1. 在开展 RFC 5011 KSK 轮转计划之前，应基于测试平台建立一组测试和衡量指标。在测试阶段应建立沟通渠道，并构建判断成功与否的评估方法。
2. KSK 轮转计划一旦可行应立即执行，重点强调准备工作。
3. 指标和监控措施是衡量 KSK 轮转的实施对技术用户和最终用户所产生影响的关键方式。
4. KSK 轮转应定期进行。
5. 应在进行 KSK 轮转之前，向各种利益相关方团体提供公开通知，以提供重要的事先通知。
6. 需要对运营稳定性、重复的 KSK 轮转，以及不符合 RFC 5011 要求的可能性和影响进行进一步的调查。

4.3 2013 年进行的根区 KSK 轮转计划初步讨论

RZM 合作伙伴于 2013 年 7 月底召开了一次会议，就开展根区 KSK 轮转的选项进行了讨论。这个团队确定了需要在保守的时间段内通过独特的步骤实施密钥轮转过程，确定了广泛的社群外展活动所带来的益处，还确定了修改包含延迟撤销的 RFC 5011 轮转计划安排的想法。在 IETF 第 87 次会议期间举行的 IETF DNS 运营 (DNSOP) 工作组会议上提出了这些高级别原则[11]。

[9] https://www.icann.org/public-comments/root-zone-consultation-2013-03-08-en
[10] https://www.icann.org/en/system/files/files/report-comments-root-zone-consultation-08apr14-en.pdf
[11] http://www.ietf.org/proceedings/87/slides/slides-87-dnsop-6.pdf

4.4 SSAC 针对 DNSSEC 根区密钥轮转计划的咨询意见

2013 年 11 月，ICANN 安全与稳定咨询委员会 (SSAC) 发布了有关 KSK 轮转计划的 SAC063[12]。报告中涵盖了所涉及的风险以及代码库当时的状态（尤其是开源 DNS 的实施）。报告建议通过沟通的方式公布根区 KSK 密钥轮转计划，鼓励通过测试来收集和分析解析程序的行为，创建指标以衡量根区 KSK 密钥轮转中可接受的“中断”级别，定义在发生过度“中断”时应采取的回滚措施，以及收集信息以便为将来的此类密钥轮转实践计划提供借鉴。

SSAC 报告着重强调了三大主题，本文稍后部分将涵盖这些主题。首先，据估计，在依赖于 DNSSEC 所支持的 DNS 的机构中，约有 1.1% 仍会受到精心管理的根区 KSK 轮转计划的负面影响。其次，DNSSEC 信任锚自动更新（也称为 RFC 5011）支持的状态已存在但不可预测。第三，如果与出现底层 UDP 包碎片并还原为 TCP 查询有关，那么 DNS 响应规模将成为一个问题。

4.5 ICANN 建立根区 KSK 轮转设计团队

2014 年 12 月，ICANN 呼吁社群志愿者与 RZM 合作伙伴一起参与设计团队的工作，以制定本文档中所展示的根区 KSK 轮转计划。

5 关于 KSK 轮转的简要说明

此项计划开始于 2013 年 7 月，与任何其他 KSK 轮转计划的开展相距不远，是在以下步骤之后制定的：

1) 生成新 KSK 密钥对（公钥和私钥）。

2) 新 KSK 公钥置于根区内和/或提供给依赖于这些密钥的各方。

3) 新的根区 KSK 公钥与其他域的不同之处在于，所有相关方真正接受其作为下一个 KSK。除被动被接受外，新的根区 KSK 公钥还通过各种电子介质和非电子介质提供，以使拥有不支持 RFC 5011 的服务器的解析器运营商和开发商有时间能够在其系统和产品中包含全新的信任锚。（对于“其他域”，此步骤改为告知 DS 记录持有者存在新 KSK。）

4) 签名过程从使用当前 KSK 私钥变为使用新 KSK 私钥。

[12] https://www.icann.org/en/system/files/files/sac-063-en.pdf

5) 新 KSK 现在处于移交状态中，因为当前 KSK 生成的签名已到期，或者由于其他原因未在运营领域显现。

6) 已从根区内移除当前 KSK 公钥（无撤销）。

7) 与正常操作的另一个差别在于，当前根区 KSK 已重新引入，以便根据 RFC 5011 准则将其标记为已撤销。这一独立步骤旨在适应 ZSK 的操作，包括轮转不含过大 DNS 响应的密钥，以提供完整的根区密钥集。

6 设计团队所采用的方法

设计团队在考量了根区 KSK 轮转计划的多个方面之后，针对调研的每个领域提出了建议，以便为根区合作伙伴制定实施计划提供指导。

- 操作注意事项：对互联网最终用户和 DNS 系统运营商的影响，以及对这些最终用户所使用的服务的影响。
- 协议注意事项：现有记录的协议元素范围是否足以满足根区 KSK 轮转计划的需求
- 对根区 KSK 管理的影响：对于 IANA 职能运营商开展 KSK 管理所涉及的流程的影响
- 加密注意事项：确保系统整体具有足够的加密强度
- 与所牵涉的各方进行沟通与协作。

在后续章节中对上述每个领域都进行了单独探讨。此外还提供了详细的技术性轮转解决方案作为如何遵循上述建议的说明，此解决方案还作为 RZM 合作伙伴最终确定其实施计划的起点。

6.1 操作注意事项

预计在以上两个步骤执行期间将对互联网最终用户和 DNS 系统运营商产生影响。在根区中添加新 KSK 公钥时，根 DNSKEY 集的响应规模将增大。当现有 KSK 私钥不再生成签名时，使用此公钥完成的验证将按预期停止工作。

随着对 DNSKEY 响应的增加，可能发生 UDP 包碎片化，并产生与 IPv4 和 IPv6 稍有不同的结果。已有某些互联网组件将碎片视为异常，并将其过滤掉。对于不保留已发送响应的状态的 DNS 而言，这意味着客户端可能无法收到期望的响应。可能较大的 UDP 响

应会超出查询指定的 DNS 有效内容缓冲区大小，从而提高被截断的响应和使用 TCP 进行后续重新查询的级别。

当现有 KSK 不再对域签名密钥进行签名时，造成的影响是新 KSK 会生成签名，而仅将现有 KSK 配置为信任锚的 DNSSEC 验证机构将无法验证已签名的 DNSSEC 响应。验证机构将“故障关闭 (fail shut)”，意味着它将把所有已签名的 DNS 响应视作为无效。

而专门使用验证解析器的最终客户无法提取新 KSK，或者无法在密钥轮转期间接收较大的响应，从而无法验证任何已签名的 DNS 响应。对于最终客户，这种现象将显示为域名无法解析的互联网中断。以前曾发生过类似的情况，由此产生的副作用是导致客户支持中心接到的呼叫数量激增，给 ISP 的客户支持和运营管理人员造成额外负担。

ICANN 应制定计划，协调有关引入新 KSK 的沟通事宜，以及从现有 KSK 切换至新 KSK 以生成签名的沟通事宜（请参阅建议 8）。

6.2 协议注意事项

6.2.1 根区信任锚配置

有两种类型的信任锚配置需要考量：

- 在线验证解析器中的信任锚
- 轮转期间脱机并稍后重新联机的设备/系统中的信任锚

在线验证解析器可以使用 RFC 5011 中所描述的 *DNS 安全性自动更新 (DNSSEC) 信任锚*，前提是所使用的 DNS 软件支持此机制，并且已配置为使用此机制来更新根区 KSK。

无法或不愿意使用 DNS 安全性自动更新信任锚的在线验证解析器将需要在 KSK 轮转期间进行手动更新。手动更新应遵循 RFC 5011 机制的时间 - 必须在轮转的“发布”期间将新的信任锚添加到此类验证解析器的配置中（请参阅第 11 部分了解详细信息），并且必须在使用新根区 KSK 签名根区之后才能删除现有信任锚。此外，为遵循谨慎操作的惯例，在撤销现有根区 KSK 之前，不应移除现有信任锚。检索新信任锚的机制与脱机设备的机制相同，如下所述。

建议 1：根区 KSK 轮转应遵循 RFC 5011 中描述的过程，在 KSK 轮转期间更新信任锚。

在根区 KSK 轮转期间脱机的设备如果在轮转完成后联机，那么将必须手动更新这些设备。尤其是必须对此类设备运行引导程序，就像安装新设备一样。

一般情况下，任何设备准备执行 DNSSEC 验证过程时都应该采用某种方法，以减少使用不适当的信任锚的机会。当前 IETF 正在标题为*“针对根区的 DNSSEC 信任锚发布”*的互联网草案中传播针对此类设备的一般建议[13]，但是需要进行更多审核，以在达成稳定共识的基础上制定出文档，为实施者提供建议。

设计团队支持社群在 IETF 内对这份互联网草案进行讨论和审核，目的是要发布一份稳定的、经过同行审查的 RFC 系列规范。

存在多个最新信任锚检索用例，以下对这些用例进行了简要描述。

6.2.1.1 对 RFC 5011 进行进一步讨论

上述文本中提到了解析器“无法或不愿意”依靠 RFC 5011 方法。本部分旨在提供有关此阶段的一些背景。

RFC 5011 的添加-保留计时器精神至关重要。包含计时器的目的是为了预防错误提供的密钥被接受。换言之就是，如果某个实体希望提供错误的 KSK，他们可能成功发布此密钥。在此情况下，真正的权威机构将能够在基于错误密钥构建任何依赖关系之前拒绝此密钥。

解析器中对 RFC 5011 的抵触并非源于更新机制设计相关的问题，而是源于一些运营现实状况。运行一组服务器并依赖于“向外推送”托管配置文件时，配置管理是主要顾虑。RFC 5011 的更新机制运行方式与之相反，已配置的机器群对新数据进行学习，这与集中托管配置截然相反。

鉴于此，大型运营商将采用手动流程，而此流程将利用多种自动化机制。其中一个自动化系统可能是一个遵循 RFC 5011 更新机制的工具。简而言之，根据非正式调研结果显示，大型运营商将采用多种不同方式来审查新的根区 KSK（包括人对人通信）来建立信任。这正是建议 RFC 5011 替代方法的原因。

通过深入分析 RFC 5011 的操作性，已经发现了一些缺陷。第一个缺陷在于对 RFC 5011 流程是否成功的远程验证。第二个缺陷在于测试有关添加-持有计时器的部署的能力。

需要一种方法来将解析器中所使用的信任锚确认为可信任的来源。考虑到普遍性监控的背景，这样做的目的并非只是了解特定解析器的配置和功能，而是首先确认已充分遵循 RFC 5011 流程，并且了解何时可以将新根区 KSK 投入使用。

[13] http://tools.ietf.org/html/draft-jabley-dnsop-validator-bootstrap-00

另外还确认了需要加快功能测试执行速度，此测试需要展示正在运行 RFC 5011 步骤，虽然这可能与所需的安全性模型不符。尤其是需要工具能够覆盖指定的添加-持有计时器，以便在测试期间缩短设置时间。提供“安全测试”机制，以确保可以接受在生产中不使用测试添加-持有计时器。这是面向工具开发人员和 DNS 软件供应商的建议。

6.2.1.2 其他信任锚格式

自从首次对根区进行签名之后，ICANN 一直通过网站提供非 DNS 格式的信任锚[14]。这些信任锚提供了一种非关键路径方法，以分发和接收根区信任锚，即，一种 DNS 运作范围之外的方法。（网站需要访问 DNS 才能获取这些文件。）根据非关键路径注意事项，可以分发新的信任锚。将来可以添加采用不同 DNSSEC 加密算法的信任锚[15]以凸显所需的新功能。这也是在由紧急情况触发的轮转之前预先填充解析器的一种方法。

6.2.1.3 DNS 软件供应商

软件供应商可能会将信任锚与其 DNS 软件（开源或专属/商用软件）打包在一起。软件供应商将不得不发布新版本的信任锚集以保持软件处于最新状态。

重要的是确保以此方式分发的信任锚是真实的，并且利用现有的任何验证机制来确保最终系统上软件的完整性。软件供应商需要健全且有效的方法来确保随其软件分发的信任锚是真实的，因为分发不真实密钥的潜在影响巨大，尤其是如果这些密钥是根据供应商软件更新策略，使用代码签名密钥来签名的，那么影响更大。

建议 2：ICANN 应确定关键 DNS 软件供应商，并与之密切协作，以制定出正式流程，确保使用特定于供应商的渠道分发信任锚是健全且安全的。

6.2.1.4 系统集成商

分发 DNSSEC 信任锚的一种方法是通过系统集成商来分发，例如，软件包维护商或操作系统供应商。在此情况下，系统集成商将为系统中信任锚的所有副本提供更新的软件包。在多个 Linux 版本中提供了具有一个信任锚权威副本的软件包。

建议 3：ICANN 应确定关键 DNS 系统集成商，并与之密切协作，以制定出正式流程，确保使用特定于集成商的渠道分发信任锚是健全且安全的。

[14] https://www.iana.org/dnssec/files

[15] https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml#dns-sec-alg-numbers-1

6.2.1.5 系统管理员

系统管理员可以在安装或更新软件时从 ICANN 的 IANA 网站手动下载 DNSSEC 信任锚。当前根区信任锚是由 IANA 职能运营商在专用网站上提供的[16]，以提供有关根区内 DNSSEC 的信息。确定下载的信任锚的真实性是在 DNSSEC 中建立信任的关键。为支持验证各种类型的数字签名的真实性，在此专用网站上还以 OpenPGP 形式发布了包含根密钥的 PKCS#7 和 X.509 证书。

虽然确定真实性至关重要，但这通常会受到忽视，并且未指明确定方式。在向公众开放真实性证明支持流程以供公众审查时收到的实质性意见很少。这对充分支持真实性的工作造成了不利影响。可能需要进一步审核（如果适用，含向后兼容改变）。如上所述，设计团队支持社群在 IETF 内对标题为*“根区的 DNSSEC 信任锚发布”*（上文中引述）的互联网草案进行讨论和审查，目的是发布稳定的、经过同行业者审查的 RFC 系列规范。

此外，支持认证的数字签名检索观察结果表明极少数（如果有）依赖于数字签名的实体会长期利用数字签名。获得信任不仅通过提供数字签名，而且来自于积极推广。

建议 4：ICANN 应积极推广适当的根区信任锚身份验证，包括强调在 ICANN 的 IANA 网站上发布的信息。

6.3 对根区 KSK 管理的影响

正如“*针对根区 KSK 运营商的 DNSSEC 实践准则*”中所述，根区 KSK 运营商利用由根区 ZSK 运营商提供的 KSR 来签署根区的每一个顶级 DNSKEY RRset。因此，将向根区维护机构提供一个 SKR，其中包含一组已签名的 DNSKEY RRset。

这些流程都已记录在案，对于在 KSK 仪式期间所采取的行动，将接受外部审计和广泛观察；设计团队认为避免因 KSK 轮转而对流程进行任何实质性更改是非常有利的，可以避免对当前广受认可的流程形式造成破坏。

建议 5：根区 KSK 轮转不应对现有流程进行任何实质性的更改，以保持与之关联的高透明度标准。

[16] 这些信息列式于以下网站：https://www.iana.org/dnssec/files

每个 KSR 均涵盖一个日历季度（三个月或约 90 天）的时间周期，并且分为 9 个时间段，每个时间段为 10 天。 如果此时间周期超过 90 天，那么周期内最后一个时间段将延长至周期结束。因此，对根区 DNSKEY RRset 进行的任何更改（例如，根据密钥轮转的要求添加和/或移除密钥）必须符合此 10 天时段，以最大限度地减少对用于发布已签名根区的流程的任何实质性更改。

建议 6：对根区 DNSKEY RRset 的所有更改都必须符合 KSK 运营商的 DPS 中所描述的 10 天的时间段。

在标准周期内，根 DNSKEY RRset 包响应大小随每个时间周期内第一个和最后一个时间段而增加。第一个时间段包含来自上一个时间周期的发布后的 ZSK，而最后一个时间段包含下一个周期的发布前的 ZSK。

为最大限度减少与较大的 DNS 响应大小相关的潜在问题，需要安排一次轮转，以尽可能保持较小的 DNSKEY RRset 响应大小。在本文稍后部分中详细解释了响应大小问题以及随附的建议。本文稍后部分中还包含了基于前述注意事项设计的根区 KSK 轮转计划。

6.4 加密注意事项

设计团队考虑了是否存在足够有吸引力的理由来考虑更改 KSK 的密钥大小或算法的问题。具有足够吸引力的理由可能来自有关所选密钥大小或算法的加密强度问题。

随着 2005 年首次发布 SP 800-57 第一部分*（密钥管理建议）*，美国国家标准技术研究所 (NIST) 宣布要提高最低加密强度。但是，在发布后直至建议的截止日期之间的五年内，因子分解技术的发展速度未达到预期。没有迹象表明根区 KSK 迫切需要使用更长的密钥。

6.4.1 有限域加密技术

2048 位非对称 RSA 密钥被视为等同于 ECRYPT II 的 2012 年算法与密钥大小年报中的 103 位对称密钥[17]。此报告还建议使用至少 96 位的安全性，以实现长达 10 年的保护。NIST *密钥管理建议 - 第一部分：常规信息 (R3)*[18] 将 2048 位 RSA 密钥视为等同于 112 位安全性，并将此强度视为可在 2014 年至 2030 年间使用的可接受强度。法国网络和信息安全局 (ANSSI) 的*通用安全框架*[19]也将 2048 位 RSA 密钥视为可用至 2030 年的安全密钥。

[17] http://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf
[18] http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf
[19] http://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf

根区中的已签名内容通常存在时间较短，因为 DNSKEY 签名周期以天来衡量（约 15 天），而设计团队相信 2048 位 RSA 密钥即使再存续 5 年也仍然是安全的，除非在大型整数分解领域出现重大技术突破。

6.4.2 椭圆曲线加密技术

可用于 DNSSEC 的另一种算法选择是 RFC 6605 中定义的椭圆曲线数字签名算法 (ECDSA)[20]。ECDSA 所包含的部分属性使之适用于作为根区 KSK 的算法。此类密钥更小，但与 RSA 密钥保持同等的强度。当前估算为采用曲线 P-256 的 ECDSA 与具有 3072 位密钥 (NIST) 或 3248 位密钥 (ECRYPT II) 的 RSA 强度相当。但直至最近才在 DNSSEC 中实现了此算法的标准化使用 - RFC 6605 发布于 2012 年 - 而本文稍后部分中所描述的度量方式经观察发现，验证机构中针对 ECDSA 的支持范围不及针对 RSA 的支持范围那样广泛（请参阅第 7 部分 - 操作注意事项）。

IETF 加密技术论坛研究小组 (CFRG) 也正在致力于全新的 *“安全性椭圆曲线”*RFC，其中添加了全新的椭圆曲线安全性，并且该小组还在加密技术社群内发表了有关 ECDSA 所使用的曲线的生成和潜在漏洞的忧虑。最好能够让 CFRG 完成有关文档的工作，然后再来处理用于根区签名的新椭圆曲线算法。

6.4.3 总结

根据上述指导意见，设计团队发现，当前不存在更改 2048 位 RSA 的 KSK 算法或大小的迫切需求。设计团队还发现，DNS 验证解析器实施计划需要使用与所配置的信任锚匹配的所有算法来完成根区签名，从而导致如果轮转为其他算法，需要采用除 KSK 轮转以外的其他算法。目前，这更进一步构成了避免更改算法的实质性动机。设计团队已就有关问题和供应商需求与供应商进行了联系，预计将来将提供不受拘束的不定期 KSK 轮转计划。

出于上述原因，首次 KSK 轮转计划的新 KSK 应为 2048 位 RSA 密钥，但是针对后续 KSK 轮转计划可能有必要考虑更改算法和/或密钥长度。

建议 7：设计团队建议针对首次根区 KSK 轮转的新 KSK 维持现有算法和密钥大小。

建议 8：对于以后的根区 KSK 轮转，应审核所选择的算法和密钥大小。

[20] https://tools.ietf.org/html/rfc6605

6.5 合作与交流

6.5.1 与技术性社群和渠道合作伙伴进行合作

ICANN 应设计并执行交流沟通计划，以提高对根区 KSK 轮转计划的认知度。应在技术性论坛内提高认知度，例如，在有关在根区内原始部署 DNSSEC 的技术论坛中。

新术语“渠道合作伙伴”指是的不参与根区管理，但推广 DNSSEC 的使用的外部组织。这些合作伙伴通过建立“渠道”，将根区签名的价值从 RZM 合作伙伴传递至全球公共互联网。

“渠道合作伙伴”分为三个一般领域。首先是支持者，即实施与 FRC 5011 的实施等事宜相关的 DNSSEC 验证软件的机构和人员。其次是软件和系统（包含 DNSSEC 验证软件）分销商，主要与分发根区 KSK 的副本有关。第三是运用根区 KSK 的 DNSSEC 验证系统运营商。

为促进沟通，设计团队建议，每个渠道合作伙伴如果愿意可以在文件中保留一名联系人的联系方式，有关 KSK 轮转计划的最新信息将发送给这些联系人。此联系人列表并非排他性列表，也并非旨在交换非公开的资料。此联系人列表旨在支持对根区 KSK 轮转计划的认知度进行采样。但应对此列表保密，以便渠道合作伙伴可以对所选联系信息的认知度加以管理。

建议 9：ICANN 应与 RZM 合作伙伴协作设计并执行沟通计划，以提高对根区 KSK 轮转的认知，包括通过适当的技术性会议与全球技术性社群进行外展活动，以及与“渠道合作伙伴”（例如，本文中指出的那些合作伙伴）进行外展活动。

6.5.2 与根服务器运营商进行合作

根区内容中的任何结构性更改都可能影响个别根服务器的运作行为。通过与根服务器运营商进行咨询和紧密协作所实现的更改包括根区内的 IPv6 地址 (AAAA) 粘合的初始配置以及 DNSSEC 的后续部署等，因为这些更改触发了查询模式的改变。因此，对待关键基础架构采取谨慎态度意味着对任何更改均采取保守态度，以防出现意外结果导致根服务器整体出现性能降级。

在本文档的准备过程中开展的实验表明，KSK 轮转事件将不会导致任何有害的效果；但是，正如上述结构性更改的示例所示，推荐采用保守性的方法。

设计团队建议个别根服务器运营商可以像处理重大计划内运营事件一样来处理 KSK 轮转期间发生的特定事件，使用用于此类事件的正常实时渠道来发布公共状态通知并与其他根服务器运营商合作。此类事件应包含将新的新 KSK 添加到根区顶级 DNSKEY RRSet，以及从该 RRSet 中删除传出 KSK 的时间段。

设计团队建议个别根服务器运营商与 ICANN 之间建立实时沟通渠道，并且在 ICANN 与其他 RZM 合作伙伴之间围绕相同事件通过类似方式来进行处理，以确保可以及时发现和分享任何期望的效果。

KSK 轮转周期的详细时间表应先经过根服务器运营商的审核，然后才能最终确定并发布，以确保与任何其他计划不存在冲突，避免导致降低个别根服务器运营商提供所期望的运营覆盖范围级别的能力。应尽可能在可行范围内努力调整轮转的时间，以避免出现运营冲突。

建议 10：ICANN 应在 KSK 轮转期间的详细时间表发布之前，要求 RSSAC 协调开展一次对这份时间表的审核，并且应提出合理的请求，以在任何根服务器运营商确定由于运作方面的原因需要修改此时间表时，对此时间表进行相应的修改。

建议 11：ICANN 应与 RSSAC 和 RZM 合作伙伴进行协调，以确保使用实时沟通渠道来保证根服务器系统能够很好地感知根区内每一次涉及添加或移除 KSK 的变化。

根服务器运营商在 KSK 轮转过程中可以通过收集数据来了解 KSK 轮转对于验证机构以及对于根服务器自身的运营影响。由于根服务器系统在架构和围绕互联网的分布方面存在多样性，因此个别根服务器运营商开展长期数据收集的机会可能受到各种约束，难以针对系统整体对这些约束加以简明扼要的概括。并且已存在基线数据收集功能用于满足在 KSK 轮转过程中实时监控服务状况的战术需求，这也是可以理解的。

当在根区中最初部署 DNSSEC 时，已开展了大量实质性的数据收集活动，在 DNS 对 DNS-OARC 推广的根区内发生的结构性更改的整体响应进行脱机分析（包括第三方分析）时，所收集的数据证明很有用。[21]。针对首次 KSK 轮转，将保证采用类似的措施。

建议 12：ICANN 应与 RSSAC 进行协调，请求根服务器运营商执行数据收集以协助后续分析，并帮助明确 KSK 轮转对运行的影响，并让第三方分析能够使用数据收集计划和结果。

[21] https://www.dns-oarc.net

6.5.3 KSK 运营商与 ZSK 运营商之间的合作

根区 KSK 和 ZSK 的管理职责分别分配给 IANA 职能运营商和根区维护机构。这两种角色各自分别接受管理。

根据 ZSK 维护机构的 DPS 中的规定，根区 ZSK 当前为 1024 位 RSA 密钥[22]。根区维护机构将来可能增加 ZSK 密钥大小。

ZSK 按 90 天的周期进行定期更新，预计在 KSK 轮转期间，仍将继续保持此状态；因为 KSK 轮转周期预计将超过 90 天，在某一段时间内，根区顶级 DNSKEY RRSet 可能包含四个密钥，具体取决于最终计划。

在密钥轮转事件期间增加 ZSK 大小可能导致在 KSK 轮转期间某一段时间内验证机构出现不同的行为，因为响应大小将随 ZSK 大小增加。这可能造成识别、了解和减轻由此出现的任何运营问题的工作变得更为复杂。

与 ZSK 大小相关的任何决策都不在本文档的讨论范围内。但是，我们建议 ICANN 与根区维护机构进行协调，确保将来增加 ZSK 大小时都与 KSK 轮转保持协调，以避免同时开展这两项实践。

建议 13：RZM 合作伙伴应确保将来增加 ZSK 大小时都要仔细考虑 KSK 轮转，以避免同时开展这两项工作。

7 对验证解析器的影响

7.1 数据包大小考量

DNS 设计为通过 UDP 和 TCP 传输协议进行操作。与 TCP 相比，UDP 开销较低，所以 UDP 更适合在设计 DNS 协议中使用，特别是在维护服务器上的连接状态时更是如此。但是，这个协议选择也有一些限制。在 DNS 的初始定义 RFC 1035 中，UDP 响应仅限于 512 个八位字节。如今，在用软件仍面临这个 512 个八位字节的限制，需履行或执行该限制。

[22] http://www.verisigninc.com/assets/dps-zsk-operator-1527.pdf

通过 DNS 的扩展机制 EDNS(0)，其最初定义是在 1999 年 8 月份出版的一个 RFC 中，[RFC 2671，由 RFC 6891 更新而来]，DNS 申请者能够通知 DNS 服务器，其可以处理大于 512 个八位字节的 UDP 响应。申请者将其最大的 UDP 负载（不是 IP 包的大小，而是 DNS 消息的大小）放入查询，并且服务器需要回复 UDP 响应，其中 DNS 负载的大小不得大于指定缓冲区的大小。如果这无法实现，则服务器会在响应中设置截位，以表明发生了截断。如果被截断的响应包括有效的 DNS 消息，申请者可以选择使用被截断的响应。否则，申请者可以打开向服务器的 TCP 会话，并通过 TCP 重复查询。

使用 DNSSEC 的 DNS 系统必须表明其能够使用 EDNS 伪首部中的 DO (DNSSEC OK) 标志来完成这个操作。本文档所考虑的运行影响全部关于支持 DNSSEC 的系统，所提及系统支持 EDNS(0)（因为 DNSSEC 需要 EDNS(0) 的支持），因此并不限定于 512 个八位字节的限制。

客户机可以在 TCP 中启动事务，但常见的申请者行为是在 UDP 中启动事务，并使用响应中的截位来表明申请者应该使用 TCP 进行查询。

在 IPv4 和 IPv6 UDP 中，数据包碎片的处理方式有所不同。如果对底层 IP 数据包传输介质而言数据包太大，可以对该 IP 数据包进行分割。在这种情况下，尾部片段使用同等 IP 级引导段（包括 UDP 协议数场），但特别排除尾部片段中的 UDP 伪首部。在 IPv4 中，原始发件人或任何中间路由器可分割 IP 数据包，除非设置*不得分割* IP 标志。在 IPv6 中，只有原始发件人可以分割 IP 数据包。如果中间路由器无法将数据包转发到下一个跳跃接口，那么在 IPv6 中，路由器将产生下一个跳跃接口中 MTU 大小的 ICMPv6 诊断包，以及数据包的主要部分，并将此信息回传给数据包的发送者。

如果使用 UDP，发送者不会维护未确认数据的缓冲区，所以 IPv6 的发送方在接收到该消息后不能重新传输原始数据。经验数据似乎表明，许多 IPv6 实现的共同响应是在本地 IPv6 转发表中生成主机条目，并且在该表中记录所接收的 MTU，以获得一些本地确定的缓存时间。这意味着在后续尝试发送 IPv6 UDP 数据包到该目的地时需要使用该 MTU 值，以确定如何分割传出数据包。

7.1.1 测量体验

设计和建立实验的目的是为了再现根服务器的环境情况，以便评估大型数据包可能对解析器和用户造成的影响。

这是通过使用在线广告平台触发 DNS 解析器，将独特的查询传送给授权域名服务器来实现的，该服务器配置为响应对两个具有不同响应大小的区域的查询。人们认为在本次测试中，那些将查询传送至授权域名服务器的解析器在很大程度上是同一组解析器，这些解析器应该查询根区域。

要测试解析器是否能接受大型响应，广告对目标域名进行了查询。目标域名本身会返回一个正常大小的响应。但是为了获取目标响应，解析器必须首先接收一个大型中间响应。如果解析器成功询问目标域名的信息，那么测试结果表明，解析器能够处理大型中间响应。

测试还涉及来自实验 Web 服务器的 Web 对象检索，帮助实验将 Web 检索所使用的地址（最终用户的 IP 地址）与构成 DNS 查询中域名解析器所使用的地址进行匹配。

该试验使用了 1,444 个八位字节的 DNS 响应。

7.1.2 测试结果

在 2015 年 5 月份的 5 天时间内，约 726 万个终端系统成功创下一个小型控制记录，而其中约 717 万个系统成功达到测试记录，约 90,000 名用户未能达到 1444 个八位字节的 DNS 测试记录，占样本系统总数的 1%。

这些终端系统使用了约 83,000 个不同的 DNS 解析器 IP 地址。其中，94% 的解析器成功创获控制记录和测试记录。在 4,251 个创获控制记录但未能检索测试记录的解析器中，3,396 个解析器通过设置 DNSSEC OK 位使用 EDNS(0) 扩展，从而触发了 1,444 个八位字节响应。在这些测试失败的解析器中，3,110 个解析器在实验期间仅出现一次故障状态，而 826 个解析器出现一次以上的故障状态。这意味着在本次实验中，1% 的解析器出现两次或更多次无法检索大型响应的情况，而另外 3% 的解析器仅出现一次未能检索大型响应的情况，这不足以断定这些服务器会始终无法检索大型响应。连续两次或两次以上发生故障的解析器占总数的 1%，使用这些解析器的终端系统不到 3,000 个，占样本终端系统总数的 0.04%。

在本次测试中，约 5,237 个解析器使用 IPv6 地址（占总数的 6%），其中 830 个解析器无法检索测试记录（占故障解析器总数的 21%）。这些数据说明一些 IPv6 解析器及其对 MTU 大小的处理存在潜在问题。

在测量大型响应查询负载的变化时，该控制名称（93 个八位字节的响应大小）经过 1640 万次查询，其中 475 次查询被观察到使用 TCP。该测试名称（1,444 个八位字节的响应大小）经过 1,860 万次查询，其中 120 万次查询是通过 TCP 进行的，约占测试名称查询总数的 6.5%。对控制记录的查询总数与对测试记录的查询总数之间存有差异。这个差异可以由通过 TCP 发送另一个查询，响应接受测试记录的截位响应的解析器进行解释。该结果与 UDP 查询的 EDNS(0) 扩展中提供的 UDP 缓冲区大小的分布存在很大的相关性。在处理大型响应时，授权服务器可以预期更高的查询负载，并且通过 TCP 进行查询的比例较高。

7.1.3 总结

约 1% 的 DNS 解析器在其查询中设置 DNSSEC OK 标志，这些解析器似乎无法收到 1,444 个八位字节的 DNS 响应（实验性不确定因素意味着这个数字最多可占所有解析器总数的 6%）。在这一系列的解析器中，使用 IPv6 作为传输协议的解析器所占比例不合理。导致这种故障率的原因是存在各种 DNS 拦截中间件，而在使用 IPv6 的情况下，原因是可能错误处理了 ICMP6 *数据包太大*消息，但故障的确切性质不能通过这种实验方法来确定。

只有少数用户的解析器未能接收响应。当涉及到此规模的 DNS 响应时，使用始终无法解析 DNS 名称的 DNS 解析器的用户占所有用户的 0.04%（实验性不确定性因素意味着这个数字最多可占所有用户总数的 1%）。

这些实验测试了 1,444 个八位字节的 DNS 响应。应当指出的是，DNS 的其他部分已经提供的响应明显大于预期规模，这些响应的大小似乎没有引起公众注意或评论。例如，2015 年 6 月 6 日针对 .org 域名的比较 DNSKEY 查询产生了 1,625 个八位字节响应，包含两个 2048 位 RSA KSK，2 个 1024 位 RSA 区域签名密钥，以及三个签名 - 一个由每个 KSK 表示，一个由一个区域签名密钥表示。无法接收如此大的 DNS 响应的任何验证解析器都将无法验证 .org 区域中每个授权的 DS 记录或 NSEC3 记录签名（用于指示不存在 DS 记录），严重导致 .org 中授权的 DNS 解析故障。

设计团队不了解 .org 中的域名持有者可能会遇到哪些与 .org 域名的 DNSKEY DNS 响应数据包大小相关的任何操作问题。即使考虑到 .org 中只有极少数的已签名区域，缺乏有关 .org 域名中解析失败的任何操作报告将表明，对于根区 KSK 轮转而言，响应大小不太可能会造成严重的操作问题。

测试用例和 .org 情况之间需要注意的一个区别是，只有实际执行验证的解析器才会查询大型 DNSKEY RRset。在此测试用例中，所有设有 DNSSEC OK 标记的解析器都会尝试获取较大的响应。如第 8.2 节中所述，在初始查询中设置 DNSSEC OK 标记的解析器中，随后执行响应验证的解析器只有不到 30%。这些开启验证的解析器运营商可能已经能够更加精炼地识别和纠正那些可能阻止他们获取大型响应数据包的任何网络问题，因为这些解析器更可能会遇到这样的问题。其他不执行验证的解析器只在极少数情况下会遇到大型响应数据包，并且可能不知道其网络环境会带来这种限制。

由此可以合理推断，绝大多数未能在测试中收到大型响应的解析器都是非验证解析器，它们将不会受到根区中 DNSKEY 资源记录大小增加的影响。

总之，这些测试表明，只有不超过 0.04% 的用户可能会在根区 KSK 轮转中受到大型响应的影响，但这个估计值含有很大的不确定因素，并且利用大型关键数据集获得的有关 TLD 的观察表明，这是大型响应的影响的上限值。[23]

7.2 DNSSEC 验证行为

可以从三个方面对 DNSSEC 验证行为进行衡量。第一个是 DNSSEC 数字签名的检索（在查询中设置 EDNS(0) 选项中的 DNSSEC OK 标志）；第二个是验证功能，其中从根密钥到正在验证的名称建立信任链；第三个是用户的域名解析配置是否会将 DNSSEC 验证失败作为明确故障予以接受，或者查询是否将被指向另一个解析器。

7.2.1 测试结果

通过以上（第 7.1.1 节）描述的实验，2015 年 5 月，大约 85% 至 90% 的用户将他们的查询传递给了解析器，其中针对未缓存域名的授权域名服务器上所观察的结果查询具有包含在查询中的 EDNS(0) 选项，还设置了 DNSSEC OK 标志。

在同一组被抽样用户中，约有 24% 的用户执行了后续查询，说明该解析器遵循联锁签名链将域名授权层次结构备份至根区 KSK，从而使用 DNSSEC 验证了响应。

在同一组被抽样用户中，约有 11% 的用户响应终端用户行为，即，通过将查询传送至另一个不执行 DNSSEC 验证的解析器，对上一次传送过来的 DNSSEC 验证失败作出响应。

这表明 DNSSEC 验证程序中的任何变化都有可能影响到约四分之一的互联网用户。

其中，将近一半的用户已经将 DNSSEC 验证失败（以 SERVFAIL 为标志）解释为将相同查询传送至另一个不执行 DNSSEC 验证的解析器的信号。对于这 11% 的被抽样互联网用户而言，根区 KSK 的变更可能包含了无法识别的根区 KSK 和验证失败，但这些用户已经表明，他们已经使用备用解析器解释了 SERVFAIL。结果可能涉及利用较长的时间来解析 DNSSEC 签名的域名，但根本不会导致无法解析该域名。

其余 13% 的用户在收到 SERVFAIL 响应时未能恢复到非验证解析器。如果他们使用的解析器无法遵循通过 RFC5011 密钥轮转过程提供的信号，那么他们很可能无法解析 DNSSEC 签名的域名。

[23] 要了解有关该实验及结果的更多详细信息，请访问 http://www.potaroo.net/ispcol/2015-05/ksk.html。

7.2.2 总结

使用这种测量方法来测试解析器是否能够遵循 RFC5011 过程，以自动选择一个新的根区 KSK 值，是根本不可能的。最好的方法是量化使用执行 DNSSEC 验证的解析器的用户群，并由此使用支持 RFC5011 或需要人工干预的解析器，在合适的时间加载新的根区 KSK。

约 24% 的用户使用执行 DNSSEC 验证的解析器，这有可能会受到根区 KSK 轮转的影响。验证失败会返回一个 SERVFAIL 响应，并且 11% 的用户会使用很多解析器，其中一个解析器发出 SERVFAIL 响应就会导致非验证解析器解析查询。这意味着，如果用户的解析器不支持 RFC5011，并且解析器管理员没有在适当的时间加载新的根区 KSK，那么，13% 的用户可能会受到根区 KSK 轮转的影响。

然而，在这些用户中，许多用户使用的是支持 RFC5011 的大型 DNSSEC 验证解析器服务（例如 Comcast 的 DNS 解析器），所以，至多会有 13% 的用户会受到影响。

8 测试

有两个因素与测试相关。一项活动是衡量 KSK 轮转对互联网常规操作的影响，进而评估可能造成操作停止的负面影响。另一项活动是关于配备操作的依赖方，包括自我测试的测试台资源。自我测试可以通过渠道合作伙伴开发软件和/或运营商部署服务器组，或任何其他感兴趣的人完成。

8.1 测试影响

针对报告中衡量验证成功部分而开展的测试已经发现了一些对 DNSSEC 验证失败的反馈。有证据表明，一些查询从 DNSSEC 开始，然后将“故障转移”到 DNS，这种做法出现的次数是否会随着 KSK 的轮转而增加（或减少）可以作为评估损害的一种方法。这种所谓的可以忽略不计的损害，可能是一种有价值的衡量指标，用于观察根区 KSK 密钥轮转操作的影响。整体而言，用户可能没有注意到这个问题，因而从未向服务提供商帮助台求助。

检测这个问题的测试应该从现在开始到根区 KSK 密钥轮转结束（成功或失败），可以定期开展关于这个问题的测试（每月一次）。在轮转之前，这种测试将会给我们提供一个比较基线。

除了自动化测试之外，在根区 KSK 密钥轮转过程中，还需要与渠道合作伙伴开展合作，以提供明确的、实时或接近实时的信息。这是一种激励因素，以便事先通知受影响的各方，在工作人员不足时避免时间跨度，并在工作人员充足时预留时间。

8.2 自我测试设备

至于授权相关方开展自我测试，应该设有测试平台，以更快的滚动速度模仿操作平台。除了具有通过已签名的伪根区更快运行 RFC5011 的服务器之外，“其他数据结构”中的信任锚也应该在同一路径中。这将鼓励开发更好的工具，例如，协助审核密钥的工具，以及发现验证器（本地或远程使用）中所含内容的工具。

这可以通过允许插入和删除不同参数的密钥，帮助开展有关新算法的教育活动。

时间是一个重要问题。对此过程的合理观察需要比实时更快的速度。但实时地进行观察也有助于降低测试的影响。

最后，必须确保对根系统的保真度，不论整个根区是否作为数据使用，或典型的伪区是否是一个考虑因素均是如此。

现有的测试台[24,25]示例可以用作将来测试的模型。

8.3 KSK 和 ZSK 维护商软件和过程修改互操作性测试

由于 KSK 轮转过程需要修改现有的时间表、过程以及可能的软件支持 KSK 操作，因此，对这些变更的全面测试必须在轮转开始之前进行，包括但不限于生成密钥、生成签名 DNSKEY RRset、验证 DNSSEC、交换 KSR/SKR、所有回退机制，以及密钥仪式彩排。

9 推行

提议的密钥轮转过程最初是在 2013 年 7 月构想的，并在之后进行了审查和完善。这里所描述的过程应该被看作是一个草案，因此，可以在实施前由 RZM 合作伙伴进一步完善。

此过程分为三个阶段：

1) 发布新的根区 KSK
2) 改为使用新的根区 KSK 进行签名（以下简称“轮转”）
3) 撤销现有根区 KSK。

[24] http://keyroll.systems/
[25] http://icksk.dnssek.info/fauxroot.html

为了支持轮转，有意推迟现有根区 KSK 的撤销，以防在将现有根区 KSK 从密钥集中移除后，新根区 KSK 出现任何问题。这个过程旨在遵循 RFC5011，利用延长的时间窗口添加新的 KSK 和撤销现有 KSK。这一过程明确允许无限期推迟撤销现有根区 KSK，以防轮转过程中出现不可预测的问题，进而需要更改密钥轮转过程计划。

下图 1 显示的是此过程在三个季度中的进展概览。请注意，季度编号是相对于过程的开始时间的，而非按照日历时间。例如，第一季度并不一定是指一月到三月。新的 KSK 称作“KSK-NEW”，现有 KSK 称作“KSK-2010”。

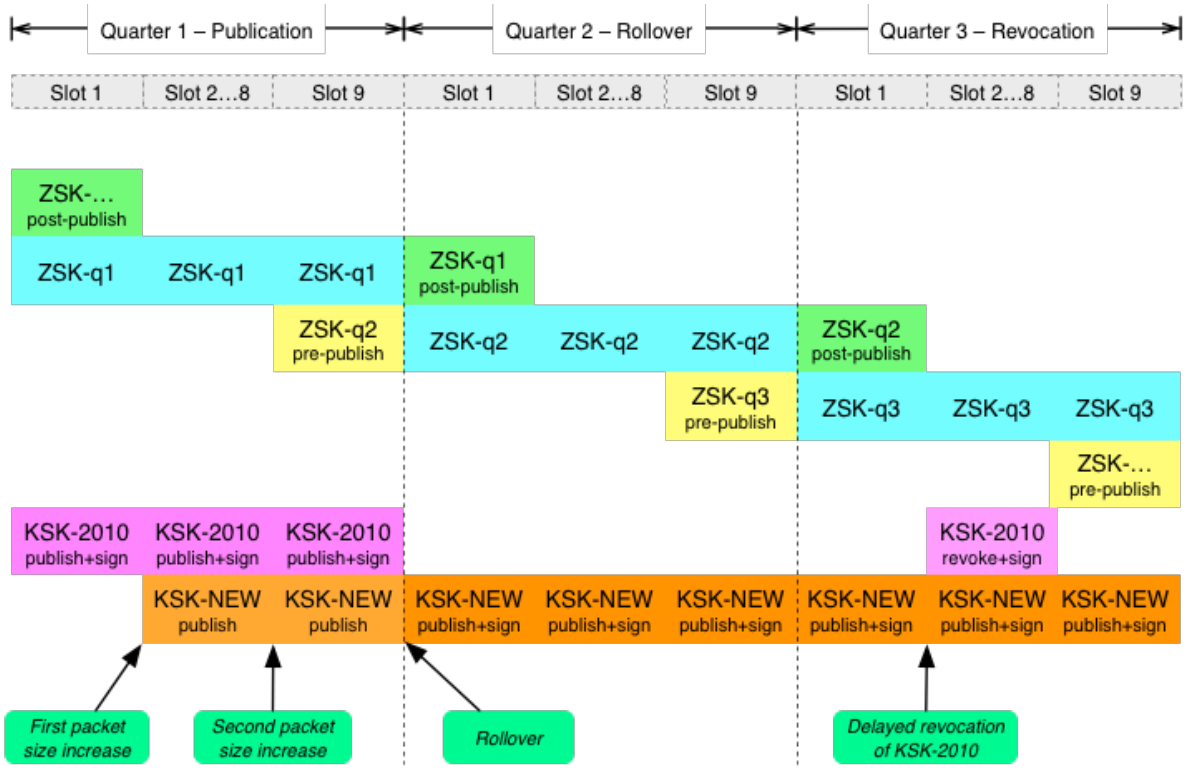

图 1.轮转计划时间安排

9.1 发布新的 KSK

新的 KSK 在第一季度的第二个时间段内添加至 DNSKEY RRset，但还不能用于签名。这是一个临时发布阶段，以便符合 RFC 5011 标准的验证器能够拾取新的 KSK。在用于签名前，新的 KSK 会在根区中公示 80 天（并由现有 KSK 签名）。在这个阶段之前或之中，会对手动配置的信任锚进行更新，以包含新的 KSK。

符合 RFC 5011 标准的轮转需要在不少于 30 天的时间内公布新的密钥（“增加抑制时间”）。如果认为提议的 80 天发布时间不够长，可以在轮转密钥前插入一个或多个其他发布季度。

在新 KSK 发布季度中，DNSSEC 验证解析器将见证对根区 DNSKEY RRset（响应数据包大小）查询的响应数据包大小由 736 个八位字节增加到 1,011 个八位字节。（在密钥轮转过程中，如果所有密钥轮转都未能达到这个大小，这个名义增长会根据此阶段中 DNS 响应大小的比较定夺。）在 ZSK 轮转第一季度的最后一个时间段内，响应数据包大小从 833 个八位字节增加到 1,158 个八位字节。

9.2 轮转到新的 KSK

新的 KSK 在引入后，从第二季度第一阶段开始即可用于对根 DNSKEY RRset 进行签名。本季度与其他季度相同，只是所有 DNSKEY RRset 均已（仅）使用新 KSK 签名。仅在可选撤销期限内，DNSKEY RRset 将由现有和新 KSK 共同签名，如下所述。

9.3 撤销现有 KSK

如果现有 KSK 按 RFC 5011 标准予以撤销，现有 KSK 将使用撤销位进行发布，并由现有和新 KSK 签名。

撤销现有 KSK 是可选的。如果需要撤销，发布已撤销的现有 KSK 要从第三季度第二阶段一直执行到第三季度第八阶段。

在撤销期间，响应数据包大小从 736 个八位字节增加到 1,297 个八位字节。

9.4 响应数据包大小的影响

所期望的目标是尽可能避免 UDP 碎片，以下是一些相关的响应大小限制：

大小	阈值
512 个八位字节	必须由 DNS 提供支持的最小 DNS 负载大小
1,232 个八位字节	未分割的 IPv6 DNS UDP 数据包中的最大 DNS 负载大小
1,452 个八位字节	未分割的以太网 IPv6 DNS UDP 数据包中的最大 DNS 负载大小
1,472 个八位字节	未分割的以太网 IPv4 DNS UDP 数据包中的最大 DNS 负载大小

表 4.数据包大小阈值

前面提到的测试结果表明，一些 IPv6 解析器及其对于大型响应的处理可能存在问题。因此，第一个和最新的大小限制是一个不可分割的 IPv6 DNS UDP 数据包的阈值，这意味着 DNSKEY 响应数据包大小最大为 1,232 个八位字节。

第一个阈值只有在可选的撤销阶段才能达到，其中现有根区 KSK 必须重新引入，并用撤销位进行标记。为完全符合 RFC 5011，这需要在撤销阶段使用新的根区 KSK 和现有根区 KSK 共同对 DNSKEY RRset 进行签名。对 RRset 进行双重签名将导致响应大小超过 1,232 个八位字节。

根区的最大单一响应数据包是已签名的 DNSKEY RRset。下表包含了提议轮转期间 DNSKEY 响应数据包大小的概述，以及与非轮转响应数据包大小的比较。

时间	轮转期间的 DNSKEY	轮转期间的 RRSIG	轮转期间的 DNSKEY 响应大小	非轮转期间的 DNSKEY 响应大小
第一季度 第一阶段	1x KSK + 2xZSK	1x KSK	883 个八位字节	883 个八位字节
第一季度第二至第八阶段	2x KSK + 1xZSK	1x KSK	1,011 个八位字节	736 个八位字节
第一季度 第九阶段	2x KSK + 2xZSK	1x KSK	1,158 个八位字节	883 个八位字节
第二季度 第一阶段	1x KSK + 2xZSK	1x KSK	883 个八位字节	883 个八位字节
第二季度第二至第八阶段	1x KSK + 1xZSK	1x KSK	736 个八位字节	736 个八位字节
第二季度 第九阶段	1x KSK + 2xZSK	1x KSK	883 个八位字节	883 个八位字节
第三季度 第一阶段	1x KSK + 2xZSK	1x KSK	883 个八位字节	883 个八位字节
第三季度第二至第八阶段	2x KSK + 2xZSK	2x KSK	1,297 个八位字节	736 个八位字节
第三季度 第九阶段	1x KSK + 2xZSK	1x KSK	883 个八位字节	883 个八位字节

表 5.轮转期间的数据包大小

（上表中的颜色编码与下图对应。）

未对与避免撤销离任密钥相关的风险进行充分探讨，但是在这个阶段，可将撤销阶段视为可选。一种选择是更新 RFC5011 中关于这方面的标准，并且不要求对撤销离任密钥进行双重签名。本次修订将具有增值效益，可以撤销遗失或消毁的密钥。无需对即将离任的密钥进行双重签名，这也可以促进未来的密钥轮转、算法变更和密钥长度变更。但是，对于此次 KSK 密钥轮转，由于重新定义、发布、开发和分发代码，以及将代码付诸操作所需的时间，因此这个选项被认为不可行。

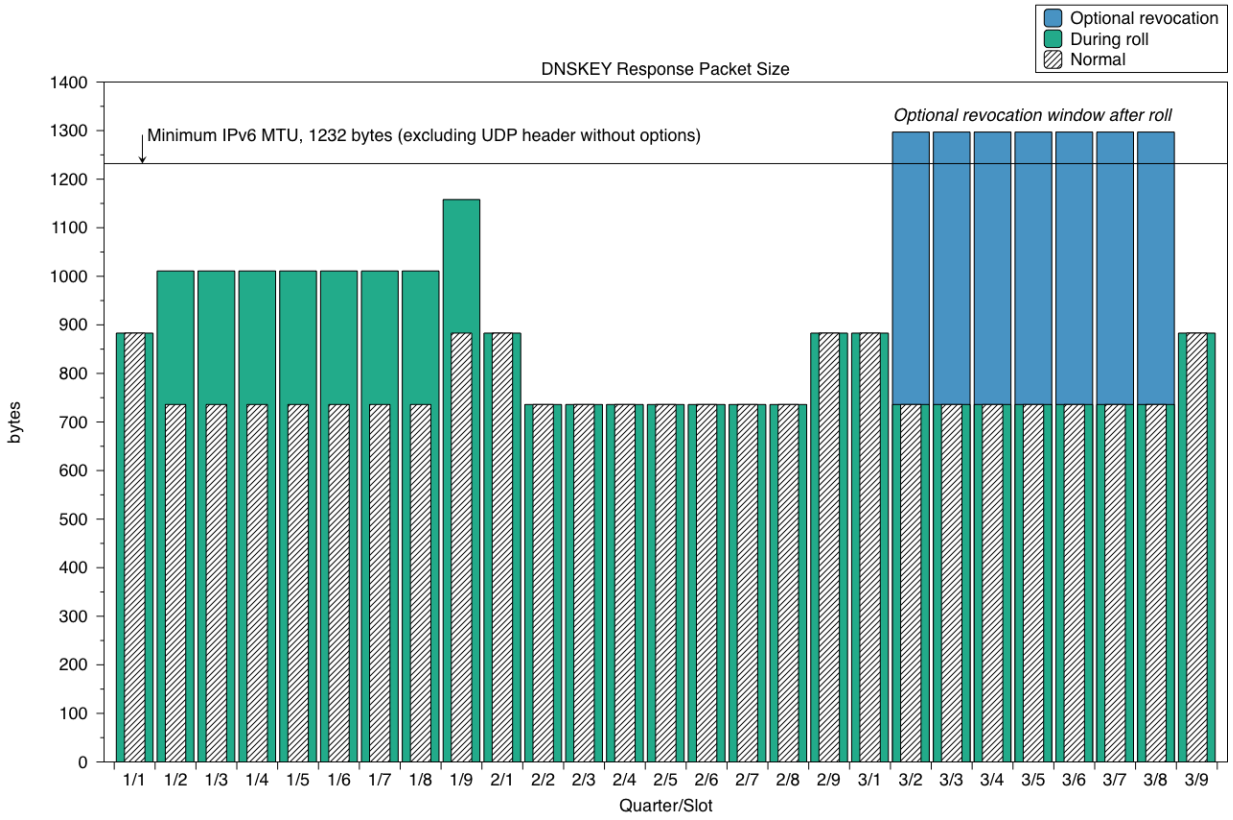

图 2.DNSKEY 响应数据包大小

9.5 逐个部署根服务器

2010 年引入 DNSSEC 是逐个根服务器进行的。2010 年 1 月，初始版本的 DNSSEC 签名区域出现在了一台服务器上；同年 2 月，出现在另一台根服务器上；3 月，出现在了另外两台根服务器上等等。我们的目标是让递归服务器（或任何将查询发送到根服务器的服务器）能够首先尝试 DNSSEC，并在答案令人无法接受时能够回退。

以前也对根区域 KSK 轮转提出过这个策略，但很快就因多方面原因被取消了。我们的目标是缓解与新根区 KSK 相关的问题，并且能够随时间推移对新信任锚的采用情况进行测评，以下这些问题阻碍了这个目标的实现。

面对 DNSSEC 验证失败，验证递归服务器的反应随工具的不同而不同。某些工具已知会在重试时积极反应，有些则不然，有些则根本不会作出任何反应。

众所周知，根本无法检测递归服务器（或任何查询来源）是否明确地选择了更合适的根服务器。一般情况下，根服务器上没有充足的查询来源跟踪用于检测递归服务器会选择哪个根服务器。每年 DNS-OARC 收集 DITL [26]的运行时间很短，这是一个巨大的工程，但仍然未能在任何时间段内设法覆盖所有根服务器。

最后要考虑的是逐步引入新信任锚可用的时间长度。在每个季度中，只有 70 天的时间位于根区 ZSK 之外。在一个 ZSK 轮转周期内，添加新 KSK（至第一个服务器）需要 40 天时间，正好剩下 30 多天来完成这项任务。最初的增量部署持续了 4 个多月。

10 回滚

如果在引入新的 KSK 后发现严重问题，那么应只准备由现任 KSK 签名的 DNSKEY RRset 进行部署。这些 RRset 是*已签名密钥响应* (SKR) 格式，因此，可以使用与非回滚 RRset 相同的根区 KSK 密钥仪式生成。此类回滚的标准还需要 RZM 合作伙伴进一步制定。

建议 14：为最大限度地缩短因涉及新 KSK 的困难所造成的恢复时间，在新 KSK 生成 SKR 的同时，当前 KSK 也应生成 SKR。

建议 15：RZM 合作伙伴应制定并记录必须使用当前 KSK 生成的 SKR 的流程。

需要为此过程的所有季度准备包含 DNSKEY RRset 的回滚 SKR。在第一季度和第二季度期间，回滚 SKR 包含具有现有 KSK 和由现有 KSK 签名的当前 ZKS 的 ZSKDNSKEY RRset 。忽略新 KSK。在第三季度中，回滚 SKR 包含具有新 KSK 和由新 KSK 签名的当前 ZKS 的 ZSKDNSKEY RRset。忽略撤销的当前 KSK。

阈值

对 DNSSEC 部署日期的测试表明，这种测试的误差范围约为 5%。这意味着，与所发生的损坏量相关的任何陈述都必须认识到 5% 的用户（个人或递归服务器 - 取决于如何进行测试）可能会在毫无察觉的情况下遭遇性能降低。由此看来，并不能将定义一个特定标准视为一种定义回滚触发器的方法。

[26] https://www.dns-oarc.net/ditl/2011

此外，目前尚不清楚会造成何种形式的损害。这可能是一个错误的部署、错误的代码应变、错误的程序或一个互联网随机行为。为此，首先需要保持与渠道合作伙伴的合作和开放问题报告渠道，然后根据判断对报告作出反应。

由于存在许多用例，除了损害的严重程度和范围之外，目前尚不清楚回滚是否还会导致除了已检测到的前进和缓解问题以外的其他损害。

11 时间

由于现有操作环境，一个日历年中有四天新根区 KSK 替代现有 KSK。这四天是每个季度的第一天，或一月、四月、七月和十月的第一天。挑选作出变化的特定日期需要考虑两个因素 - 什么是合理操作，以及什么与目前有关 IANA 移交的讨论相符。[27]

合理操作是指所涉及的日期应避开影响工作安排的周末和节假日，以及操作人员工作内容安排得较满的时间。由于在挑选这三个日期时需要考虑全球用户，因此，可能无法满足所有条件。另一个难题是，在 2016 年和 2017 年，每个季度的第一天都是周五、周六或周日。在 2018 年之前，每个季度的第一天都是如此。（2015 年第四季度中，10 月 1 日是星期四，但此时计划还未实施，更不需要完成测试以在那天进行密钥轮转了。）

非技术性影响是计划的 IANA 管理权移交。这会导致此时无法建议具体日期。

12 风险分析

12.1 准备不充分造成的风险

描述	影响	可能性	缓解措施
利益相关方认为，具有相同算法、哈希和大小的 KSK 滚动更新将不够充分	低	不可能	第一次轮转结束后立即计划另一次轮转；如果需要不同的参数，直接更改即可
网络运营商将不知道变更（即，NOC 获取故障票证，需要知道如何作出反应）	中	可能	在沟通计划中，运营商予以关注

[27] http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

描述	影响	可能性	缓解措施
网络运营商和软件开发商（或“所有渠道合作伙伴”）将没有（无法获得）充分的测试环境	中	可能	设置具有加速和即时轮转的 ICANN RFC5011 测试平台；其他测试
无法在过程中集中进行测试	低	可能	制定分布式测试方法；拟定联系人列表
缺少作出推进/不推决定的决定性标准	低	可能	需要准备通信和测试；对现场所用机制的可行性研究；需要长期努力开发对更新后信任锚验收工作的度量

12.2 自动化信任锚机制无效或不充分

描述	影响	可能性	缓解措施
未执行 RFC5011 的情况随处可见	中	可能	备用信任锚管理办法
RFC5011 未完全执行	中	不可能	联系软件开发商；验证对 RFC5011 的理解
验证程序引导过程未完全执行	中	不可能	联系系统集成商和信任锚处理商
ICANN 的 IANA 网站未提供信任锚集合	低	不可能	可用性监控
由于缺乏维护，设备未同步信任锚集合	低	可能	沟通计划

12.3 移除现有 KSK 导致验证失败

描述	影响	可能性	缓解措施
（所有过程参与者）未能充分遵循自动化信任锚协议	低	可能	检测，通信；为运营商提供资源以加速修复
由于“故障后重试功能”，导致流量增加	低	不可能	检查“轮转后失效[28]”的持续影响；消极的缓存建议

12.4 添加新的 KSK 会导致 DNS 信息大小超过限制

描述	影响	可能性	缓解措施
密钥集的转换会生成过大的数据报	中	不可能	通过检查消息大小制定周详的转换计划
混淆 DNS 软件中的 IPv6 碎片处理	低	不可能	检查并测试 DNS 软件

12.5 发生操作失误

描述	影响	可能性	缓解措施
拙劣的 KSK 轮转会终结采用 DNSSEC 的趋势	高	不可能	精心设计/评审
在紧急情况下无限期推迟密钥轮转会加大影响	高	不可能	致力于根区 KSK 轮转
一旦开始，永远不能返回到当前的可接受状态	高	不可能	制定回退计划

[28] http://iepg.org/2010-03-ietf77/dnssec-goes-wrong.pdf，http://www.potaroo.net/ispcol/2010-02/rollover.html

未能充分摧毁现有 KSK（专用组件）	低	不可能	承诺完成计划

13 设计团队成员名单

13.1 社群志愿者

- 加利福尼亚州 (CA) Dyn Inc. 的 Joe Abley
- 荷兰 (NL) NLNetLabs 的 Jaap Akkerhuis
- 英国 (UK) Sinodun Internet Technologies 公司的 John Dickinson
- 澳大利亚 (AU) APNIC 的 Geoff Huston
- 捷克 (CZ) CZ.NIC 的 Ondrej Sury
- 荷兰 (NL) No Hats/Red Hat 的 Paul Wouters
- 日本 (JP) JPRS 的 Yoshiro Yoneya

13.2 根区管理合作伙伴

- ICANN David Conrad
- ICANN Edward Lewis
- ICANN Richard Lamb
- ICANN Alain Durand
- ICANN Hayley Laframboise
- ICANN Elise Gerich
- ICANN Kim Davies
- ICANN Roy Arends
- ICANN Jakob Schlyter
- ICANN Fredrik Ljunggren
- 威瑞信 Brad Verd
- 威瑞信 Duane Wessels
- 威瑞信 David Blacka
- 威瑞信 Al Bolivar
- US DoC NIST 的 Tim Polk
- US DoC NIST 的 Scott Rose
- US NIST 的 Doug Montgomery
- US DoC NTIA 的 Ashley Heineman
- US DoC NTIA 的 Vernita Harris

14 参考资料

- RFC 5011：DNS 安全 (DNSSEC) 信任锚的自动化更新
  https://tools.ietf.org/html/rfc5011
- SAC063：SSAC 关于根区 DNSSEC 密钥轮转的公告
  https://www.icann.org/en/system/files/files/sac-063-en.pdf
- 《适用于根区 KSK 运营商的 DNSSEC 实践准则》
  https://www.iana.org/dnssec/icann-dps.txt
- 《适用于根区 ZSK 运营商的 DNSSEC 实践准则》
- https://www.verisigninc.com/assets/dps-zsk-operator-1527.pdf
- 根区 DNSSEC 信任锚公布
  https://tools.ietf.org/html/draft-jabley-dnssec-trust-anchor
- 在启动时建立合适的根区 DNSSEC 信任锚
  https://tools.ietf.org/html/draft-jabley-dnsop-validator-bootstrap

15 附录：渠道合作伙伴

术语“渠道合作伙伴”是指独立支撑或传递管理根区 KSK 的价值的外部组织。这些组织与 RZM 合作伙伴没有正式建立合作关系，但在一定程度上的合作是必不可少的。每个组织应维护适当的联系信息，以沟通与根区 KSK 变更有关的状态和其他信息。

渠道合作伙伴的排列不分先后顺序。

15.1 软件生产商

与这些合作伙伴的实质性交流涉及是否在软件中实施了 RFC5011 信任锚管理。这组合作伙伴需要验证递归缓存服务器。本文档中未列出这些组织的联系信息。

- ISC 的 BIND (http://www.isc.org)
- NLNetLab 的 Unbound (https://nlnetlabs.nl)
- Microsoft Windows Server (https://www.microsoft.com/)
- Nominum 的 Vantio (http://nominum.com/caching-dns/)
- DNSMASQ (http://www.thekelleys.org.uk/dnsmasq/doc.html)
- IRONSIDES (http://ironsides.martincarlisle.com)
- Infoblox (http://www.infoblox.com/)
- Secure64 DNS 缓存 (http://www.secure64.com/)

15.1.1 待定事项

以下这组合作伙伴已经讨论但尚未公布 DNSSEC 验证递归缓存服务器。如果代码已发布，这些服务器就位于要包含在内的列表中。（不支持 DNSSEC 的 其他 DNS 递归缓存服务器不依赖于根区 KSK）

- CZ.NIC 的 TBD 递归服务器（除节点外）
- PowerDNS TBD

15.2 系统集成商

这些渠道合作伙伴将根区 KSK 作为涉及上述 DNS 软件配置数据的一部分进行传输。人们的期望是，这些机构将审查新的根区 KSK，并将其纳入他们的软件更新中。

15.2.1 Linux

- Red Hat Enterprise Linux (RHEL) RPM
- Micro Focus International 公司的 SUSE (RPM)
- Fedora
- CentOS
- Debian 和 Canonical (Ubuntu) APT
- Montavista Linux

15.2.2 BSD

- FreeBSD ports
- NetBSD pkgsrc
- OpenBSD ports

15.2.3 其他

- Apple iOS、OS X
- Google Android、ChromeOS
- Microsoft
- Cisco
- Juniper
- Belkin
- Cisco/Linksys
- Wind River (RTOS)
- QNX (RTOS)
- OpenVMS
- OpenWRT

15.3 公共解析器运营商

据报告，这些合作伙伴运行递归 DNS 服务器，在某些情况下，还验证 DNSSEC。我们希望这会将根区 KSK 作为配置数据包含在内，因此可能需要进行内部审核以了解新根区 KSK。

- Google Public DNS
- OpenDNS
- Neustar DNSAdvantage
- Symantec ConnectSafe
- 3 级

- Censurfridns
- Comodo
- Dyn Internet Guide
- Liquid Telecom

以上所列的公共解析器运营商是根据接受互联网中任意位置流量的情况选出来的（到目前为止可以看出），除此之外，其他运营公共解析器的合作伙伴对他们依赖的合作伙伴群有所限制。这些合作伙伴已经过确认，他们也将收到有关根区 KSK 事件的通知。