根区 KSK 轮转展望

ICANN 首席技术官办公室

2018 年 8 月 22 日

执行摘要

根区 KSK 轮转启动（当前计划时间：2018 年 10 月 11 日）后，预计一小部分互联网用户将在解析某些域名时遭遇困境。目前，少量验证递归解析器的域名系统安全扩展 (DNSSEC) 配置错误，依靠这些解析器解析域名的部分用户势必出现问题。本文介绍哪些用户将会遇到问题，以及不同时期将会面临哪些类型的问题。

- 如果用户依靠解析器但不执行 DNSSEC 验证，那么将不会因轮转而受到任何影响。
- 如果用户依靠解析器且获取新的 KSK，也不会因轮转而受到任何影响。
- 如果所有用户解析器的信任锚配置中均不具备新 KSK，那么在轮转后的 48 小时内，用户可能会陆续感受到影响。
- 究竟受影响解析器的运营商何时会发现无法执行验证，则根本无从预测。
- 据数据分析显示，99% 以上需要执行解析器验证的用户不会因 KSK 轮转而受到影响。

1.简介

早在多年前，ICANN 组织已经公布即将对 DNS 根区 KSK 进行轮转。[1]在最近一次修订轮转计划的公共评议期内，[2]很多社群成员询问轮转流程细节。ICANN 组织同意发布更多材料，帮助做好轮转准备工作。[3]为此，我们发表了这篇文章。

一直以来，很多不同社群对轮转后将会（将不会）引发的状况存在一定的困惑。本文自轮转启动的一刻起开始进行详细预测。

本文的读者多种多样。主要分为以下三类：

- 希望在轮转后了解查询目标的解析器验证运营商
- 非技术出版物或希望在轮转前期和中期创作相关资料的其他各方
- 监控 DNS 确定轮转后是否存在解析器解析失败的研究人员

值得注意的是，使用至少一个做好轮转准备的解析器的各方也可能对本文略感兴趣。完成轮转后，这些用户将会发现，DNS 或互联网整体使用均不存在任何变化。对于解析器完全不执行 DNSSEC 验证的用户而言，情况也是如此。据目前估计，2/3 的解析器用户并未执行 DNSSEC 验证。

目前计划将于 2018 年 10 月 11 日进行轮转。KSK 轮转日期尚待 ICANN 董事会表决，然后才会进行轮转。起初计划于 *2017* 年 10 月 11 日进行轮转，但因轮转前收到的数据尚不清晰，所以被迫延期。[4]

[1] http://www.icann.org/kskroll
[2] https://www.icann.org/public-comments/ksk-rollover-restart-2018-02-01-en
[3] https://www.icann.org/en/system/files/files/report-comments-ksk-rollover-restart-23apr18-en.pdf

本文的第 2 和第 3 部分介绍轮转后验证轮转专用解析器及非专用解析器的过程。第 4 部分介绍监控 DNS 根服务器系统流量的研究人员可能遇到的状况。整篇文章并未使用任何非确定性短语介绍轮转后的情形。之所以这样说，是因为没人比解析器运营商更能精准定位哪款软件由其解析器运行，也没人更能准确判断解析器是否针对轮转正确配置。

解析器运营商重要说明：在读到本文后，全体解析器验证运营商应立即检查其当前的信任锚，验证是否做好轮转准备。[5]如果运营商尚未做好准备，应尽早更新至最新信任锚。[6]尚未执行 DNSSEC 验证的解析器运营商已做好轮转准备。

1.1 根区 KSK 轮转定义

早在 2010 年，我们已通过 DNSSEC 对 DNS 根区进行了签名。DNS 根区共包含两种密钥：签署根区主数据的域签名密钥 (ZSK) 和签署根区的根区密钥集（包括 ZSK 和 KSK）的密钥签名密钥 (KSK)。每隔三个月发布一次新 ZSK。每个新 ZSK 均经过长期有效的 KSK 签名。

当根 KSK 发生更改且新的 KSK 开始对根区的根区密钥集进行签名时，则将进行轮转。轮转期间，原始 KSK 将被停用，新 KSK 取而代之。第一个 KSK 称为 KSK-2010（至今仍在使用）。新 KSK 称为 KSK-2017。轮转后，KSK-2010 将不再对根区密钥集进行签名，KSK-2017 将转而执行根区密钥集签名。

1.2 信任锚

为了解轮转流程，掌握验证解析器如何对根区 KSK 表示信任同样至关重要。每个验证解析器均通过一组*信任锚*进行配置。信任锚是与根区 KSK 匹配的密钥或密钥标识符副本。信任锚通常由软件供应商自动配置、由配置按照 RFC 5011 中所述的流程自动更新信任锚的解析器配置，[7]或者由手动向解析器信任锚存储区添加新 KSK 的解析器运营商配置。

在 KSK-2017 问世之前，所有验证解析器仅配置 KSK-2010 作为信任锚。创建并发布 KSK-2017 后，大部分解析器运营商要么手动将 KSK-2017 添加至解析器信任锚配置，要么通过其软件（如通过 RFC 5011 自动更新流程）或软件供应商做出调整。但是，有些解析器运营商并未更新其配置，由于仍然使用 KSK-2010 作为信任锚，眼下对轮转显得束手无策。一旦进行轮转，这些解析器运营商将不具备有效信任锚。

2.做好轮转准备的解析器

做好轮转准备的解析器已配置 KSK-2017 作为信任锚。当进行轮转时，这些解析器将继续保持轮转前的状态运行，因为新的根区 KSK 已获得信任，可以对根区密钥集进行签名。某些解析器软件可能会在发生轮转的运行日志进行标识，但除非运营商刻意查询，否则不太可能看到这些日志条目（如果存在）。

---

[4] https://www.icann.org/news/announcement-2017-09-27-en
[5] https://www.icann.org/dns-resolvers-checking-current-trust-anchors
[6] https://www.icann.org/dns-resolvers-updating-latest-trust-anchor
[7] https://datatracker.ietf.org/doc/rfc5011/

轮转期间，准备进行轮转的解析器用户看不出任何不同。轮转前后，执行常规查询获得的响应完全相同。据最近一次 APNIC 研究发现，[8]99% 以上的用户在通过解析器执行 DNSSEC 验证时所使用的解析器已做好轮转准备。

大部分互联网用户配置了多个 DNS 解析器。如果用户配置的任何解析器已做好轮转准备，用户软件应在轮转后找到该解析器并继续使用。这可能会减缓 DNS 解析速度，因为他们的系统会一直尝试调用未做好准备的解析器，然后才会切换至准备妥当的解析器，但用户仍可完成 DNS 解析。

3.未做好轮转准备的解析器

如果解析器仅配置 KSK-2010 密钥作为信任锚，经过轮转后，解析器将无法再验证从权威服务器获得的响应。但是，验证失败的起始时间无从预测。

虽然 DNS 发布瞬间完成，但解析器发现新发布的记录可能存在时间延迟。每一条 DNS 记录都具有“存活时间”（通常称为 *TTL*），在此期间，解析器将不会尝试获取新版记录。经过轮转后，解析器很可能仍具有 KSK-2010 生成的缓存版签名，因而仍可顺利完成验证，至少暂时如此。

3.1 无法验证 ZSK 时开始发生失败

每当验证解析器获得权威域名服务器的响应，都会检查响应签名。将每个域名的签名验证状态保存到其缓存中。为验证域名（如 www.example.com）签名，解析器需要在根区、.com、example.com 和 www.example.com 上验证签名。通常，解析器会对这些验证进行缓存，避免每次执行验证。大部分解析器仅在验证状态可能发生变化时执行验证。

KSK 和 ZSK 记录的 TTL 为 48 小时。如果解析器*刚好*在轮转前获取根区密钥集并进行验证，就在大概两天前，解析器还对轮转一无所知，因为在根区密钥集 TTL 到期且执行首次查询之前，解析器不会获取新的 KSK。在仅有少数几位用户的常规解析器中，将在 DNSKEY 记录 TTL 到期后几分钟（乃至几秒钟）内触发查询。在只有一位用户的解析器中，根区密钥集的 TTL 到期后，可能需要数小时（乃至数天）才可能触发首次查询。

请注意，相较于实际情况，这种描述略微有些轻描淡写。例如，某些解析器采用最大 TTL 长度，这样解析器可以在较短的时间内完成密钥轮转。其他配置选择也可能影响解析器首次进行轮转的时间。

3.2 用户在所有解析器失败后将会经历的场景

在完成解析的 48 小时内，某些用户的 DNS 查询将开始失败，因为他们需要使解析器再次获取根区密钥集。如上所述，用户无法预测在这 48 小时内的哪一个时刻将会发生首次失败。

发生此类失败后，倘若与大部分用户一样，这位用户配置了多个解析器，系统软件将尝试调用用户配置的其他解析器。这可能会减缓 DNS 解析速度，因为他们的系统会一直尝试调用未做好准

[8] http://www.potaroo.net/ispcol/2018-04/ksk.html

备的解析器，然后才会切换至准备妥当的解析器，但用户仍可完成 DNS 解析，很可能对迟钝一无所知。但是，如果所有用户的解析器均未做好轮转准备（例如，所有解析器均通过一家组织管理，并且该组织的所有解析器均未做好准备），用户将于轮转后的 48 小时内开始出现解析失败现象。

用户失败症状各不相同，具体取决于他们运行的程序及该程序对 DNS 查询失败做出的响应。浏览器网页很可能不再可用（或者，也可能已显示的网页上的唯一图像无法显示）。在电子邮件程序中，用户可能无法接收新邮件，或者部分邮件正文可能显示错误。失败将持续涌现，直至任何程序均无法显示新的互联网信息。

请注意，此处的术语“用户”不仅仅是指人类。如果自动化系统同样采用未准备就绪的解析器执行 DNS 解析，那么也会开始发生失败，而且很能遭受毁灭性打击。

解析器运营商修复验证缺陷（要么添加 KSK-2017 作为信任锚，要么关闭验证），用户的互联网体验几乎立即恢复正常。

3.3 解析器运营商如何发现失败

倘若解析器运营商已配置系统监控软件查找重大错误，那么在解析器获取新的根区密钥集副本但无法执行验证后将立即收到提醒。上述监控是一次大好良机，运营商可趁机快速检测失败并予以恢复。

如果运营商未主动监控最大错误，可能无从了解发生失败的验证，直至依靠该解析器运行的自动化系统开始发生失败，或者用户开始反映中断问题。如果运营同样仅使用信任锚配置错误的解析器，则可能收不到向其发送的电子邮件，只能通过电话获悉发生问题。

3.4 从无准备情况下恢复正常

一旦运营商发现其解析器的 DNSSEC 验证发生失败，应更改解析器配置，暂时禁用 DNSSEC 验证。这样可以即刻杜绝问题。

而后，运营商应尽快安装 KSK-2017 作为信任锚并再次启用 DNSSEC 验证。ICANN 组织就更新常用解析器软件的信任锚提供了说明。[9]

4.根服务器运营商的未来

经过轮转后，根服务器运营商将渐渐发现，来自未做好轮转准备的解析器的查询大幅增加。其中以根 DNSKEY (./IN/DNSKEY) 查询居多，同时还可能包括 .net 根区的 DS 记录 (.net/IN/DS) 查询。此外，鉴于无法正确验证响应，将无法进行缓存，进而导致来自这些验证解析器的总体流量增加。同样，如果解析器运营商允许其他解析器通过其传递信息，那么很可能在轮转后发现此类请求的数量有所增加。

[9] https://www.icann.org/dns-resolvers-updating-latest-trust-anchor

研究人员已开始监控根服务器流量的根 DNSKEY 请求，以便对每分钟查询数进行基本了解。在 12 家根服务器组织中，有 11 家近实时（每分钟一次）向 ICANN 报告这些统计数据。轮转开始后，ICANN 将继续监控这些统计数据，再将结果报告给根服务器运营商及其他 DNS 技术社群。

附录 A. 了解更多轮转资讯的资源

主要轮转信息来源如下所示：

http://www.icann.org/kskroll

此页面不仅提供了 KSK 轮转快速指南、大量 DNSSEC 相关资源，还介绍了社群选择轮转的原因及轮转计划。本页面还以英语、西班牙语、法语、俄语、阿拉伯语、中文、葡萄牙语、韩语和日语等多语呈现。

订阅以下电子邮件清单，参加轮转讨论：

https://mm.icann.org/listinfo/ksk-rollover

附录 B. 词汇表

DNSSEC – DNS 扩展，允许权威服务器对 DNS 记录进行加密签名，从而使解析器确信记录数据未经改动。[10]

KSK (Key Signing Key) – 密钥签名密钥，用于对一个根区内的所有密钥进行签名的密钥。

轮转 – 更改根区内的密钥签名密钥，使其从现有密钥改为新密钥。

TTL (Time To Live) – 一组 DNS 记录的“存活时间”。当解析器从权威服务器获取一组记录时，通常会将这些记录保存至缓存，保存时间为 TTL 中所示的秒数。

验证 – 验证受 DNSSEC 保护的根区记录的签名。解析器执行验证，以便确保从权威服务器获取的记录准确无误。

ZSK (Zone Signing Key) – 根区签名密钥，用于签署根区内的所有记录（而非密钥）的密钥。签署密钥的密钥为密钥签名密钥。

[10] https://meetings.icann.org/en/marrakech55/schedule/sun-dnssec-everybody