根区密钥签名密钥 (KSK) 轮转

KSK 轮转概览

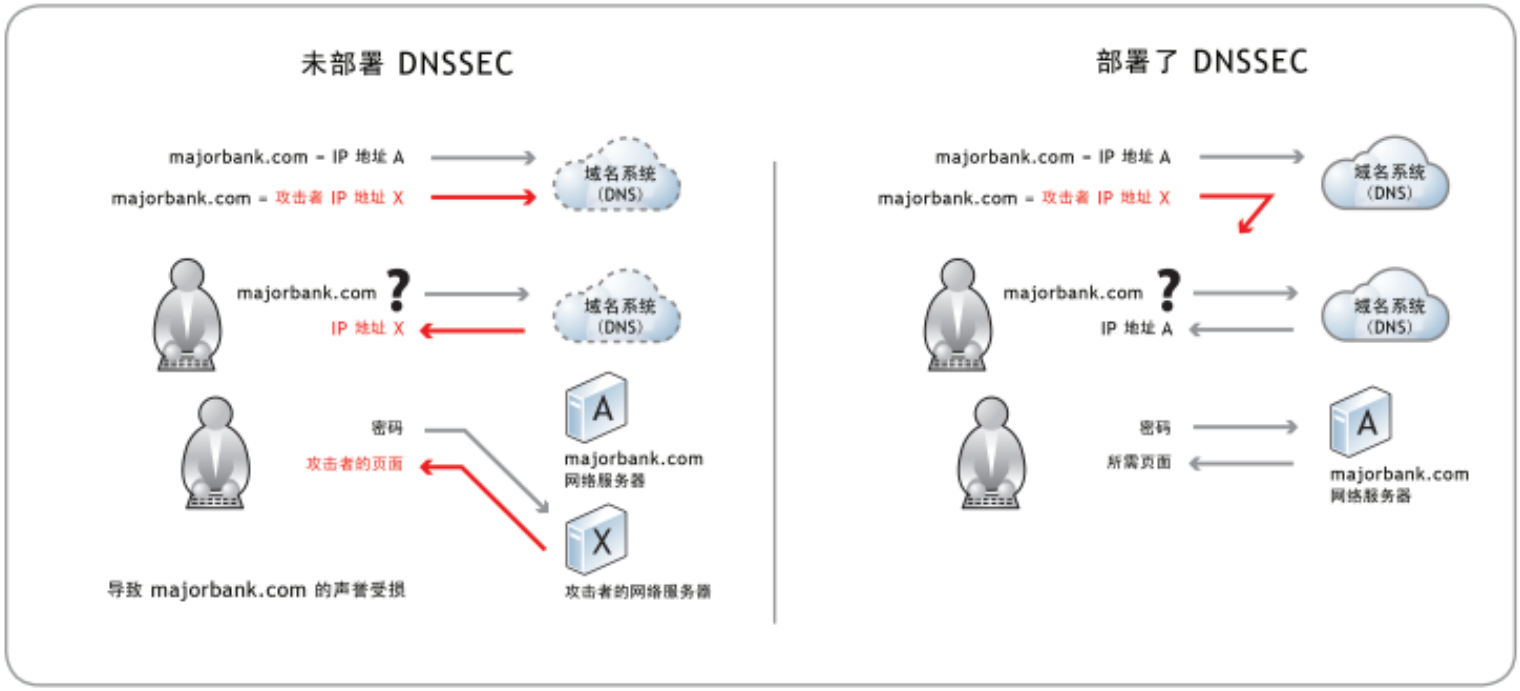
ICANN 正计划对用于域名系统安全扩展 (DNSSEC) 协议（俗称根区 KSK）的“顶级”加密密钥组进行轮转或变更。这将会是 KSK 自 2010 年最初生成以来的首次变更。

变更 DNSSEC 密钥是一个重要的安全措施，如同任何互联网用户定期改变密码被视为谨慎的做法一样。

根区 KSK 包含一个私钥和一个公钥。私人组件由 ICANN 安全地保存着，但是公共组件广泛分布和配置在数以百万计的大量设备中。多步骤 KSK 轮转流程主要包括生成一对新的加密密钥并分配新的公共密钥。

互联网服务提供商、企业网络运营商和其他 DNSSEC 验证实施者必须确保其系统更新为新 KSK 的公共组件，以确保其用户可顺利访问互联网。

KSK 是 DNSSEC 的必要构成部分，而 DNSSEC 是验证域名系统 (DNS)（互联网的全球电话本）内信息完整性的安全技术。这种变更以前从未发生在根级，因此必须在大范围内谨慎地协调轮转，以确保其不干扰正常运营。鉴于此，现在 ICANN 正趁轮转并未真正开始前通知互联网运营商和用户社群该变更。



KSK 在 DNSSEC 中发挥着什么作用？

KSK 的重要作用体现在通过验证 DNS 数据，保护互联网用户免遭域名劫持。顾名思义，域名劫持即控制域名，通常为带有恶意且寻求非法经济利益的人所为。例如，试图获取他人银行账户信息的人可能使用户重定向到一窃取身份和密码的网站.

KSK 轮转为什么至关重要

KSK 已广泛分配至实施 DNSSEC 验证的每一位运营商。如果 KSK 轮转时使用 DNSSEC 的验证解析器没有新的密钥，基于这些解析器的终端用户将遇到错误且无法访问互联网。

根区 KSK 是公共密钥链（验证解析器用于确认 DNS 数据的真实性）中的第一个密钥。密钥链起始处从根 KSK 开始的各密钥都为下一个密钥的有效性提供担保。如果根区 KSK 发生变更但解析器配置未更新，密钥链中的首个密钥将是错误的，从而使整个密钥链都无效。因此 DNSSEC 验证将失败，而产生的错误将使用户无法访问互联网。

轮转什么时候开始？

KSK 轮转是一个过程，而非单一事件，预计将于 2018 年 3 月完成。新的公共密钥暂定于 2017 年 2 月发布于 http://data.iana.org/root-anchors/，并将于 2017 年 7 月 11 日首次出现在 DNS 中。

下面是轮转流程中的一些其他里程牌。请注意，这些日期可能由于运营考量进行更改：

- **2016 年 10 月：**生成新 KSK
- **2017 年 2 月：**在 IANA 网站上发布新 KSK
- **2017 年 7 月：**在 DNS 中发布新 KSK
- **2017 年 10 月：**将新 KSK 用于签字（实际轮转事件）
- **2018 年 1 月：**撤销旧 KSK
- **2018 年 3 月：**销毁旧 KSK 并完成 KSK 轮转流程

多少人会受到影响？

预计全球四分之一的互联网用户或 7.5 亿人都可能受到 KSK 轮转的影响。该数字是基于使用 DNSSEC 验证解析器的互联网用户的估计数量得出的。

谁需要采取行动？

强烈建议支持 DNSSEC 验证的软件开发商支持 RFC 5011 信任锚自动更新协议。代码或配置文件中包含根区 KSK 的软件开发商和经销商应确保使用新根区 KSK，最好在新 KSK 于 2017 年 2 月发布后尽快使用。

基于 RFC 5011 信任锚自动更新协议的运营商应确保其支持 DNSSEC 的解析器配置为轮转发生时自动更新根区信任锚。手动更新支持 DNSSEC 的解析器信任锚配置的运营商应确保新根区 KSK 在 2017 年 10 月 11 日前配置完成。

任何编写、整合、发布或运行支持 DNSSEC 验证且完全符合 RFC 5011 信任锚自动更新协议的软件的人员都无需采取任何行动。

资源

提问

要提交问题，请发送电子邮件至 globalsupport@icann.org，并在主题栏中标示“KSK 轮转”字样。

详细了解 KSK 轮转

https://www.icann.org/kskroll

参与对话

通过话题标签 #KeyRoll：https://twitter.com/icann