快速指南：
准备系统以进行根区 KSK 轮转

什么是根区 KSK 轮转？

互联网名称与数字地址分配机构 (ICANN) 计划轮转或更换在域名系统安全扩展 (DNSSEC) 协议中使用的“顶级”加密密钥对，此加密密钥对通常称为根区密钥签名密钥 (KSK)。这将是 KSK 在 2010 年最初生成以来的第一次更换。此次更换被认为是一项重要的安全举措，就像定期更换密码被看作是互联网用户的谨慎之举一样。

更换密钥需要生成新的加密密钥对，并将新的公共组件分发给 DNSSEC 验证解析器。由于每个使用 DNSSEC 的互联网查询都依赖于根区 KSK 来验证目标，因此，这将是一项重要的变更。新的密钥现已生成，运营商（例如 ISP）需要使用新密钥更新他们的系统，以便当用户尝试访问网站时，可以根据新的 KSK 对用户进行验证。

为什么需要准备系统

目前，全球互联网用户中大约有四分之一通过 DNSSEC 验证解析器来访问互联网，这些用户会受到此次 KSK 轮转的影响。如果在轮转 KSK 后，这些验证解析器没有新密钥，依赖于这些解析器的最终用户将会遇到错误，并且无法访问互联网。

如果您不使用 DNSSEC，您的系统将不会受到轮转的影响。不过，您应该知道 DNSSEC 是防止域名劫持的重要组件。

ICANN 提供了一个测试平台，运营商或任何相关方可以使用这个平台确认他们的系统能否正确处理自动更新过程。通过访问以下网址，可检查以确保您的系统准备就绪：**https://go.icann.org/KSKtest**。

如果您启用了 DNSSEC 验证，必须使用新 KSK 更新您的系统，以帮助确保用户能够顺利访问互联网。

需要完成的工作

可以使用 2017 年 7 月 11 日发布的新根区 KSK，在轮转之前的任何时间更新您的系统，有些系统可能已经自动更新。您需要采取的操作取决于以下方面。

如果您的软件支持自动更新 DNSSEC 信任锚 (RFC 5011)：

将在适当的时间自动更新 KSK。您无需执行其他操作。

请注意，在轮转期间脱机的设备如果在轮转完成后联机，那么必须手动更新这些设备。

ICANN 从 2017 年 3 月起提供了一个测试平台，运营商或任何相关方都可以使用这个平台来确认他们的系统能否正确处理自动更新过程。如需了解更多信息，请访问 **https://icann.org/kskroll**。

如果您的软件不支持自动更新 DNSSEC 信任锚 (RFC 5011)，或者未配置为使用此信任锚：

必须手动更新软件的信任锚文件。可在以下位置获取新根区 KSK：**https://go.icann.org/2DOB7zn**。

何时进行 KSK 轮转？

KSK 轮转是一个过程，而非单个事件。以下日期是轮转过程中的重要里程碑，最终用户可能会在这些日期遇到互联网服务中断情况：

2018 年 10 月 11 日

第一次使用新 KSK 进行签名的提议日期。

2019 年 1 月 11 日

撤销旧 KSK 的提议日期。

如需了解有关轮转的更多信息，包括可帮助您为即将进行的密钥更换做好准备的资源，请访问 **https://icann.org/kskroll**。

您也可以发送电子邮件至 **globalsupport@icann.org**，并在主题行中注明“KSK 轮转”，或者使用 #KeyRoll 加入 Twitter 上的对话。