KSK 轮转：常见问题与解答

什么是密钥签名密钥？

- 根区密钥签名密钥 (KSK) 是一对加密公/私钥，在域名系统安全扩展 (DNSSEC) 中发挥着重要作用。根区 KSK 是 DNSSEC 验证受信任的起点，如同根区是 DNS 解析的起点一样。

- 正如软件从根区开始对 DNS 中任意位置的域名进行解析一样，执行 DNSSEC 验证的软件信任根区 KSK 并创建后续密钥和签名的“信任链”，以验证 DNS 中任何签名数据的真实性。

密钥签名密钥 (KSK) 轮转涉及到什么？

- KSK 轮转流程将新的 KSK (KSK-2017) 引入根区，以更新根区信任锚。

为什么要轮转 KSK？

- 因为始终保持加密密钥不变是不利的。与任何密码一样，密钥需要不时进行更改。
- 与其当出现紧急情况时被动更改，不如当一切运行顺畅时，在正常操作中主动进行更改。
- 2010 年首次部署 DNSSEC 时，NTIA 要求轮转 KSK，接着根区管理合作伙伴提出了每运行五年更改一次密钥的要求。NTIA 的角色已于 2016 年 10 月 1 日结束。

哪些人需要知晓 KSK 轮转？

- 互联网服务提供商、企业网络运营商和其他 DNSSEC 验证管理方，必须使用新密钥签名密钥的公共部分更新其系统。

他们如何获知 KSK 轮转信息？

- ICANN 正在开展广泛的外展活动，以确保当前使用 KSK 的人知晓相关更改。

- 相关方可在 ICANN 网站上查看包括轮转讨论的议程，还可跟进 KSK 进展及加入特殊电子邮件清单。相关方还可在社交媒体上跟进话题标签 #KeyRoll 来了解最新进展。

对互联网用户有何影响？

- 如果顺利完成，终端用户将不会感受到明显变更。

可能出现什么问题？

- 某些执行 DNSSEC 验证的软件可能不会进行新 KSK 的更新，或者某些软件可能无法处理发布在 IANA 网站上的信任锚文件中的变更。如果这些复杂情况普遍存在，根区管理合作伙伴可决定撤销变更，以使系统恢复至稳定状态。这称为“撤销情况”。如有必要，例如若新信息表明下一阶段可能出现复杂情况，可延长特定阶段的时长，以确保稳定性。

“撤销”或延时有什么影响？

- 撤销或延时的要点在于维持运行稳定性，使得对终端用户的影响降至最低。

撤销或延时将持续多久？

- 可能无限期地持续，或直到研究出导致撤销的原因并予以纠正为止。纠正操作将被并入新的 KSK 轮转流程。

KSK 到底将如何轮转？

- 轮转将分为八个阶段进行，预计需要两年左右。各个阶段都涉及到一个预定的密匙仪式。

- KSK 对 DNSKEY 资源记录组 (RRset) 进行签名，RRset 均为根区中特定域名的记录。这些签名在密钥签名仪式期间生成，将成为签名密钥响应 (SKR) 的一部分。

八个阶段的时间安排是怎样的？

- **阶段 A：密钥生成（2016 年 10 月）**
  - KSK-2017 在首个安全密钥管理设施中生成
- **阶段 B：密钥复制（2017 年 2 月）**
  - KSK-2017 被复制至第二个安全密钥管理设施中。此时 KSK 可进入生产状态。
- **阶段 C：使用 KSK-2017 对首个数据进行签名，以用于阶段 D（2017 年 5 月）**
  - 对首个密钥签名请求组进行签名。
- **阶段 D：发布（2017 年 8 月）**
  - KSK-2017 发布至根区。
  - KSK-2010 和 KSK-2017 均用于对根区进行签名。
- **阶段 E：轮转（2017 年 11 月）**
  - 仅 KSK-2017 用于对根区进行签名。
- **阶段 F：撤销（2018 年 2 月）**
  - KSK-2010 从根区移除。
- **阶段 G：删除 1（2018 年 5 月）**
  - KSK-2010 从首个安全密钥管理设施中删除。
- **阶段 H：删除 2（2018 年 8 月）**
  - KSK-2010 从第二个安全密钥管理设施中删除

目前可采取什么行动？

- 创建或维护 DNSSEC 验证软件的软件开发人应确保软件符合 RFC 5011。

- 对于不符合 RFC 5011 的软件，或配置为不使用 RFC 5011 的软件，点击此处可获得发布流信任锚文件。一旦开始轮转且 DNS 根区中 DNSKEY RRset 的 KSK 发生变更，即应检索文件。
- 软件开发人和验证解析器运营商可进行 ICANN 开发的运营测试，评估其系统是否恰当执行 RFC 5011 的要求及是否将在 KSK 轮转期间自动更新。