Roulement de la KSK des extensions de sécurité du système des noms de domaine (DNSSEC)

FRATEL 2018
Antananarivo, Madagascar

Yaovi ATOHOUN

ICANN

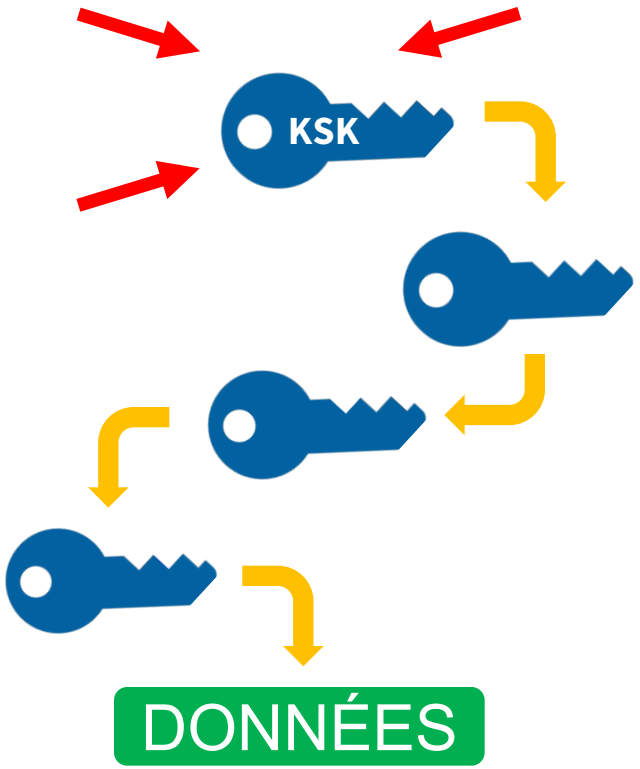
Roulement de la KSK : un aperçu

L'ICANN prépare le roulement de la clé de signature de clé (KSK) des extensions de sécurité du système des noms de domaine (DNSSEC)

- La clé de signature de clé « **KSK** » des DNSSEC de la zone racine est la clé cryptographique qui se trouve au sommet de la hiérarchie des DNSSEC.

- La KSK est une paire de clés cryptographiques publique-privée :
  - Partie publique : point de départ fiable pour la validation de DNSSEC.
  - Partie privée : signe la clé de signature de zone (ZSK).

- Construit une « chaîne de confiance » des clés et des signatures successives afin de valider l'authenticité des données signées avec DNSSEC.



Pourquoi l'ICANN change-t-elle la KSK ?

- Parce ce qu'il n'est pas souhaitable qu'une clé cryptographique reste inchangée pour toujours. Les clés cryptographiques utilisées pour signer avec DNSSEC les données du DNS doivent être régulièrement modifiées.
  - Cela permet de s'assurer que l'infrastructure est capable de supporter le changement de clé en cas d'urgence.

- Ce type de changement ne s'est jamais produit au niveau de la zone racine.
  - Depuis 2010 il n'y a eu qu'une seule et même KSK opérationnelle et fonctionnelle pour les DNSSEC de la zone racine.

- Parce qu'il est préférable d'apporter des changements proactifs pendant les opérations normales, quand tout se passe bien, plutôt que d'être réactif en cas d'urgence. Le roulement doit être largement et soigneusement coordonné pour s'assurer qu'il n'interfère pas avec les opérations normales.

DNSSEC

Quand le roulement de la KSK a-t-il lieu ?

- Le changement ou « roulement » de la KSK était initialement prévu pour le 11 octobre 2017, mais il a été retardé car certaines données obtenues en septembre 2017 ont montré qu'un grand nombre de résolveurs utilisés par les fournisseurs de services Internet (FSI) et les opérateurs de réseau n'étaient pas encore prêts pour le roulement de la clé.

- Il y a plusieurs raisons qui expliquent pourquoi les opérateurs n'ont pas la nouvelle clé installée dans leurs systèmes : certains n'ont peut-être pas configuré correctement le logiciel de leurs résolveurs.

- Après une consultation préliminaire avec la communauté, l'ICANN a publié un plan pour redémarrer le processus de roulement. Ce plan a été ouvert à la consultation publique à l'https://www.icann.org/public-comments/ksk-rollover-restart-2018-02-01-en. **La période de commentaires a pris fin le 2 avril 2018 et de l'ICANN prépare un résumé.**

- Le plan vise à ce que l'ICANN change la clé de signature de clé (KSK) le 11 octobre 2018 et encourage les FSI et les opérateurs de réseau à utiliser ce délai supplémentaire pour s'assurer que leurs systèmes sont prêts pour le roulement de la clé.

Qui sera affecté ?

Développeurs et distributeurs de logiciels DNS

Intégrateurs de systèmes

Opérateurs de réseau

Opérateurs de serveurs racine

Utilisateurs finaux
(si pas de mesures prises par les opérateurs des résolveurs)

Pourquoi devez-vous être préparé ?

Si vous avez activé la validation DNSSEC, vous devez mettre à jour vos systèmes avec la nouvelle KSK pour garantir que les utilisateurs n'auront pas de problèmes pour accéder à Internet.

- À l'heure actuelle, 25 % des utilisateurs mondiaux d'Internet, soit **750 millions de personnes**, utilisent des résolveurs validant les réponses avec DNSSEC qui pourraient être affectés par le roulement de la KSK.

- Si ces résolveurs ne sont pas configurés avec la nouvelle clé lors du roulement de la KSK, les utilisateurs finaux qui en dépendent rencontreront des erreurs et **ne pourront pas accéder à Internet**

Que doivent faire les opérateurs ?

Vérifier si la validation DNSSEC est activée dans vos serveurs

Vérifier comment la confiance est évaluée dans vos opérations

Tester/vérifier vos configurations

Contrôler les fichiers de configuration, sont-ils (aussi) à jour ?

Si la validation avec DNSSEC est activée ou prévue dans votre système

- Planifier votre participation au roulement de la KSK ;
- Connaître les dates, les symptômes, les solutions.

Comment mettre à jour votre système

Si votre logiciel prend en charge les mises à jour automatiques des ancres de confiance des DNSSEC (RFC 5011) :

- La KSK sera mise à jour automatiquement, le moment venu
- Il n'est pas nécessaire de prendre d'autres mesures
  - Les dispositifs qui sont hors ligne durant le roulement devront être mis à jour manuellement s'ils sont mis en ligne une fois que le roulement est terminé

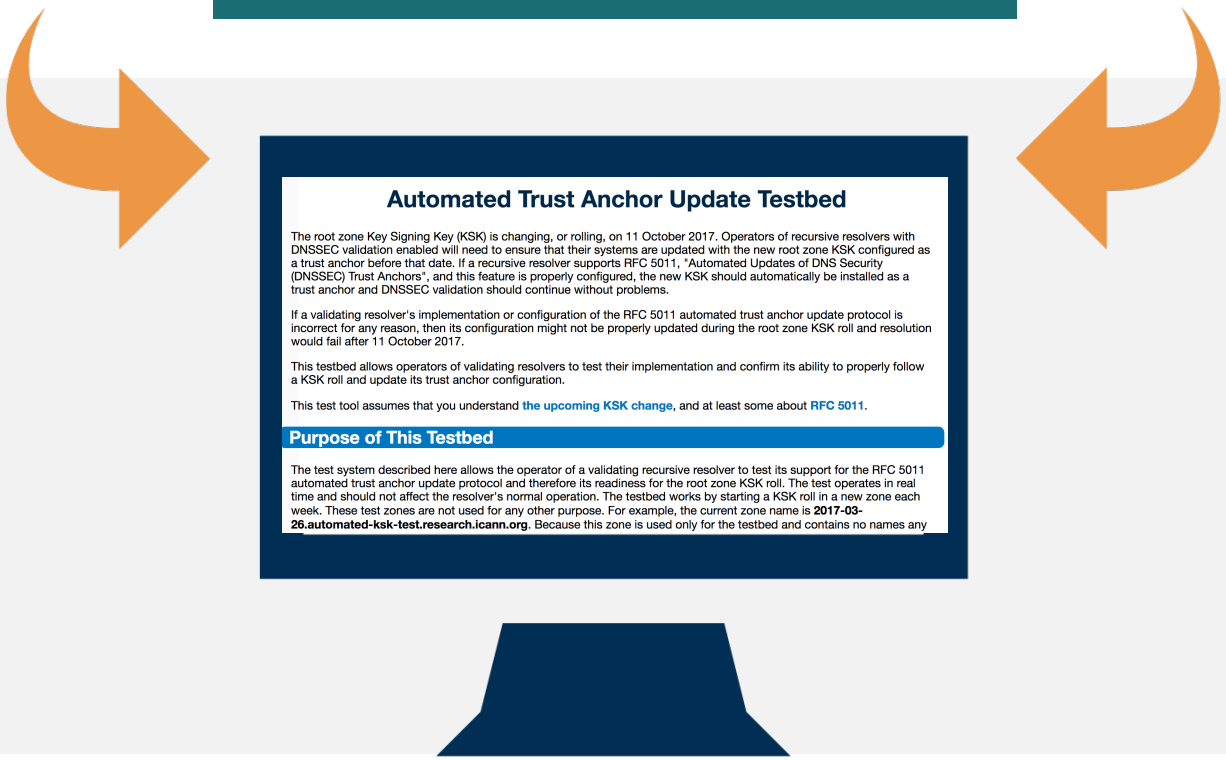
Si votre logiciel <u>ne</u> prend <u>pas</u> en charge les mises à jour automatiques des ancres de confiance des DNSSEC (RFC 5011) ou s'il n'est pas configuré pour les utiliser :

- Le fichier de l'ancre de confiance du logiciel doit être mis à jour manuellement
- La nouvelle KSK de la zone racine est maintenant disponible ici après mars 2017 :
  http://data.iana.org/root-anchors/

Vérifiez pour voir si vos systèmes sont prêts

L'ICANN propose un **banc d'essai** pour les opérateurs ou toute autre partie souhaitant s'assurer que leurs systèmes peuvent gérer correctement le processus de mise à jour automatique.

Vérifiez pour vous assurer que vos systèmes sont prêts à l'adresse suivante :
go.icann.org/KSKtest



Trois étapes de la récupération

Si votre validation DNSSEC est défaillante après le roulement de la clé :

Arrêter les tickets

Il est possible de désactiver la validation DNSSEC jusqu'à ce que le problème soit résolu (mais pensez à la réactiver après !)

Déboguer

Si le problème est l'ancre de confiance, cherchez à comprendre pourquoi elle n'est pas correcte.

- Le RFC 5011 n'a-t-il pas été correctement mis en œuvre ? Les outils de configuration n'ont-ils pas réussi à mettre à jour la clé ?
- Si le problème est lié à la fragmentation, vérifiez que le TCP est activé et/ou faites d'autres ajustements au niveau du transport.

Vérifier la récupération

Assurez-vous que vos corrections fonctionnent.

Pour plus d'information

1. **Visitez https://icann.org/kskroll**

2. **Rejoignez les conversations en ligne**
   - utilisez le hashtag #KeyRoll
   - Inscrivez-vous à la liste de diffusion https://mm.icann.org/listinfo/ksk-rollover

3. Envoyez vos questions à **globalsupport@icann.org**
   - Ligne objet : « Roulement de la KSK »

4. **Assistez à un événement**
   - Consultez https://features.icann.org/calendar pour trouver les prochaines présentations sur le roulement de la KSK dans votre région