

4. Le processus de roulement de la KSK de la zone racine de l'Internet

L'ICANN s'apprête à entamer une opération majeure pour la sécurité de l'Internet à l'échelle mondiale, en procédant à la modification de la paire de clés cryptographiques publique- privée, à savoir la clé KSK de la zone racine. Cette opération s'appelle « roulement de la KSK ».

Ce roulement implique la création d'une nouvelle paire de clés cryptographiques qui sera utilisée dans le processus de validation de DNSSEC.

S'agissant du 1^{er} changement de cette clé **KSK-2010** (la zone racine a été signée en 2010), et en vue d'éviter tout incident pouvant nuire à la stabilité de la zone racine de l'Internet et par conséquent au fonctionnement de l'Internet dans le monde entier, ICANN a prévu un planning progressif, permettant aux acteurs concernés de se préparer à ce roulement important.

5. Les principaux acteurs concernés par ce changement

« Rouler » la KSK signifie générer une nouvelle paire de clés et distribuer sa nouvelle composante publique aux parties qui opèrent les résolveurs validant DNSSEC, y compris les fournisseurs de services Internet, les administrateurs de réseaux d'entreprise, les développeurs de logiciels de résolveurs du DNS et les distributeurs de matériel et de logiciels qui installent la clé publique de la KSK de la zone racine.

Il est donc essentiel d'obtenir la nouvelle clé publique de la KSK de la zone racine afin de veiller à ce que les noms de domaine continuent à être validés après le roulement. A défaut, les résolveurs validant DNSSEC seront incapables de vérifier que les réponses du DNS n'aient pas été faussées et retourneront donc une réponse d'erreur pour toutes les requêtes validées par le DNSSEC.

Ces résolveurs doivent s'assurer de la conformité de leurs systèmes avec la **RFC 5011**.

Dans ce cadre, l'ICANN a mis en œuvre une plateforme de tests permettant aux acteurs précités de tester que leurs systèmes peuvent supporter ledit roulement. Voir <https://automated-ksk-test.research.icann.org/>.

6. Nouvelle date annoncée par l'ICANN pour effectuer le roulement de la clé KSK

L'ICANN ayant reporté le roulement de la clé KSK, initialement prévu pour le 11 octobre 2017, a programmé ce roulement pour le 11 octobre 2018.

Aussi, et dans le cadre des actions de sensibilisation menées par l'ICANN à ce sujet, un guide a été mis en ligne sur : <https://www.icann.org/news/announcement-60-2018-08-27-fr>. Ce guide est mis par l'ICANN à la disposition de la communauté Internet en vue de lui permettre de bien assimiler ce processus de roulement.

Pour plus de détails sur le roulement de la KSK de la zone racine, voir également : <https://www.icann.org/resources/pages/ksk-rollover>.