



# Roulement de la clé de signature de clé (KSK)

**BENIN DNS Forum,  
15 Octobre 2016 | Cotonou – Benin**

Pierre Dandjinou, VP Stakeholder Engagement - Africa

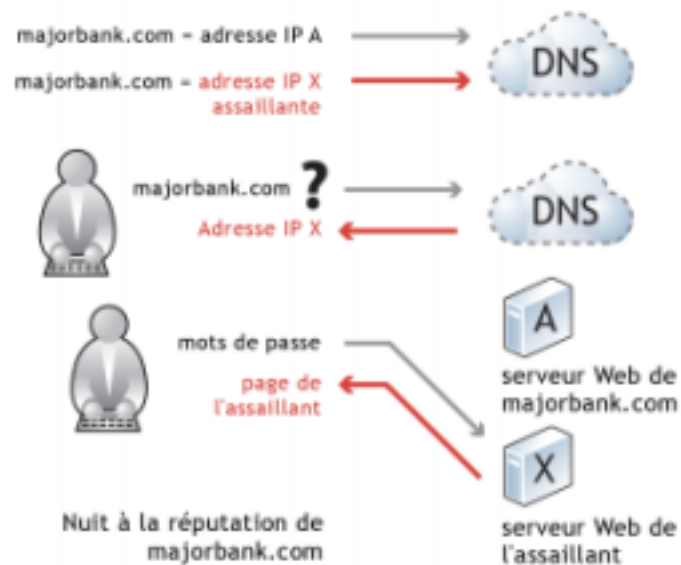
# Rappel sur le DNS

Chaque ordinateur connecté à Internet dispose d'une adresse numérique unique (semblable à l'unicité d'un numéro de téléphone) qui représente une chaîne de nombres difficile à mémoriser pour la plupart des utilisateurs. Cette chaîne s'appelle l'« adresse IP ». IP est l'acronyme d'« Internet Protocol ».

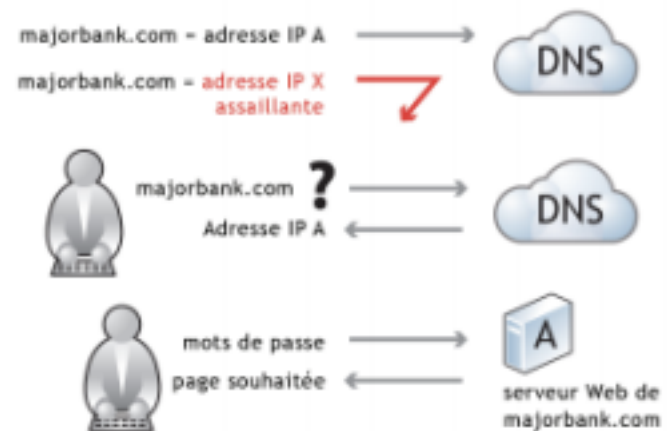
Pour faciliter la recherche d'un site donné sur Internet, le système de noms de domaine (DNS) a été inventé. Le DNS traduit les adresses IP en adresses alphanumériques uniques appelées noms de Domaine.

# La sécurisation du DNS par le DNSSEC

## Sans DNSSEC



## Avec DNSSEC



# La clé de signature de clé (KSK)

La KSK (Key Signing Key) est une composante essentielle de DNSSEC (Domain Name System Security Extensions) , une technologie de sécurité qui authentifie l'intégrité de l'information dans le système des noms de domaine (DNS), qui est l'annuaire téléphonique mondial de l'Internet

# Roulement de la clé KSK

L'ICANN a l'intention de rouler, ou modifier, la paire « principale » de clés cryptographiques utilisée dans le protocole des extensions de sécurité du système des noms de domaine (DNSSEC), communément dénommé la KSK de la zone racine . Ce sera la première fois que la KSK aura été changée depuis qu'elle a été initialement générée en 2010.

# Dates importantes du processus de roulement

- ❑ Octobre 2016 : génération de la nouvelle KSK
- ❑ Février 2017 : publication de la nouvelle KSK sur le site web de l'IANA
- ❑ Juillet 2017 : publication de la nouvelle KSK dans le DNS
- ❑ Octobre 2017 : la nouvelle KSK utilisée pour signer (le cas de roulement à proprement parler)
- ❑ Janvier 2018 : révocation de l'ancienne KSK
- ❑ Mars 2018 : destruction sécurisée de l'ancienne KSK et achèvement du processus de roulement de la KSK



Les fournisseurs de services Internet, les opérateurs de réseaux d'entreprise et d'autres acteurs chargés de la validation de DNSSEC doivent assurer que leurs systèmes soient mis à jour avec la partie publique de la nouvelle KSK afin d'assurer à leurs utilisateurs l'accès à Internet exempt de perturbations.

- ❑ Pour poser une question  
veuillez envoyer un courrier électronique à  
[globalsupport@icann.org](mailto:globalsupport@icann.org) en mettant « roulement de la KSK »  
dans la ligne objet du message.
- ❑ Apprenez davantage sur le roulement de la KSK  
<https://www.icann.org/kskroll>
- ❑ Participez au débat  
Utilisez le hashtag #KeyRoll : <https://twitter.com/icann>



# Engage with ICANN



## Thank You and Questions

Reach us at:

Email: [engagement@icann.org](mailto:engagement@icann.org)

Website: [icann.org](http://icann.org)



[twitter.com/icann](https://twitter.com/icann)



[gplus.to/icann](https://plus.google.com/icann)



[facebook.com/icannorg](https://facebook.com/icannorg)



[weibo.com/ICANNorg](https://weibo.com/ICANNorg)



[linkedin.com/company/icann](https://linkedin.com/company/icann)



[flickr.com/photos/icann](https://flickr.com/photos/icann)



[youtube.com/user/icannnews](https://youtube.com/user/icannnews)



[slideshare.net/icannpresentations](https://slideshare.net/icannpresentations)