SEMINAIRE FRATEL
8-9 mai 2017, Abidjan –Cote d'Ivoire

Table ronde 3 Enjeux relatifs au fonctionnement technique de l'internet

Quelques ressources critiques dans la sécurité Internet

Yaovi Atohoun, ICANN

Agenda

- ICANN en bref
- Les Adresses IP et le DNS
- La transition IPv4-IPv6
- Sécurité du DNS - Roulement de la KSK de la zone racine
- Conclusion

L’ICANN EN BREF

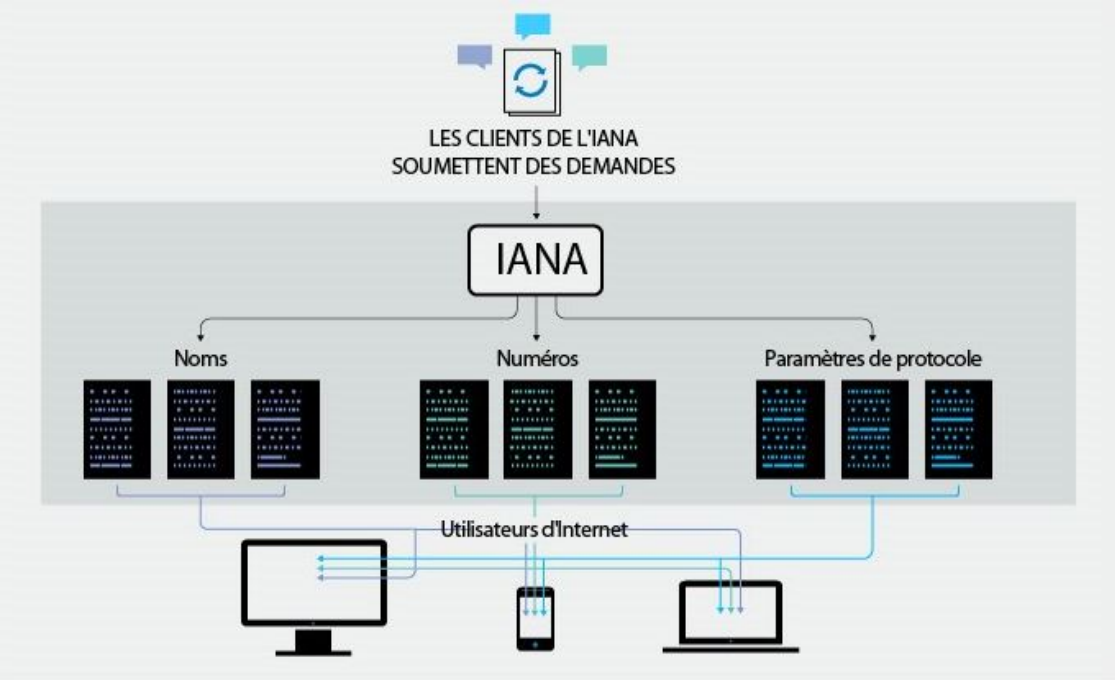
Qu'est-ce que l'ICANN ?

La Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN) est une organisation multipartite mondiale du secteur privé qui gère les ressources Internet dans l'intérêt du public

- L'ICANN coordonne le premier niveau du système d'identifiants uniques d'Internet au moyen de processus politiques globaux et multipartites, basés sur un consensus ascendant, et dont les résultats sont mis en application par les fonctions IANA.

En quoi consistent les fonctions IANA ?

Les fonctions IANA ont évolué afin de soutenir le Groupe de travail de génie Internet (IETF). À l'origine, elles étaient financées par des projets de recherche soutenus par l'Agence pour les projets de recherche avancée, qui dépend du Département de la défense des États-Unis.



Ces fonctions incluent :

- La coordination de l'attribution des paramètres de protocoles techniques d'Internet
- L'administration de certaines tâches associées à la gestion de la zone racine du DNS
- L'attribution des adresses IP d'Internet

L'ICANN a été créée en 1998 notamment pour exécuter les fonctions IANA

Les composantes de l'ICANN

L'ICANN comprend trois parties :

La communauté de l'ICANN est un groupe de parties prenantes issues du monde entier qui travaillent ensemble à titre bénévole pour donner des conseils et élaborer des politiques dans le cadre de la mission de l'ICANN.

Le Conseil d'administration de l'ICANN est un groupe de représentants de la communauté de l'ICANN qui supervise l'organisation ICANN.

L'organisation ICANN met à disposition de la communauté et du Conseil d'administration de l'ICANN des effectifs et des ressources, et met en œuvre les politiques élaborées par la communauté.

Les bureaux de l'ICANN

Appelez un de nos bureaux régionaux ou posez vos questions en ligne. Visitez-nous sur : **icann.org/contact**

Bureaux régionaux :

Los Angeles, USA (Quartier général)
Istanbul, Turquie
Montevideo, Uruguay
Singapour

Bureaux de liaison :

Beijing, Chine
Bruxelles, Belgique
Genève, Suisse
Nairobi, Kenya
Séoul, République de Corée
Washington, D.C., USA

Partenariats :

Asunción, Paraguay
Le Caire, Égypte


Les Adresses IP et le DNS

Les adresses IP

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 ».

- Deux versions d’adresses IP: Ipv4 et IPv6
- AFRINIC (www.afrinic.net) alloue les blocs d’adresses IP pour la région AFRIQUE

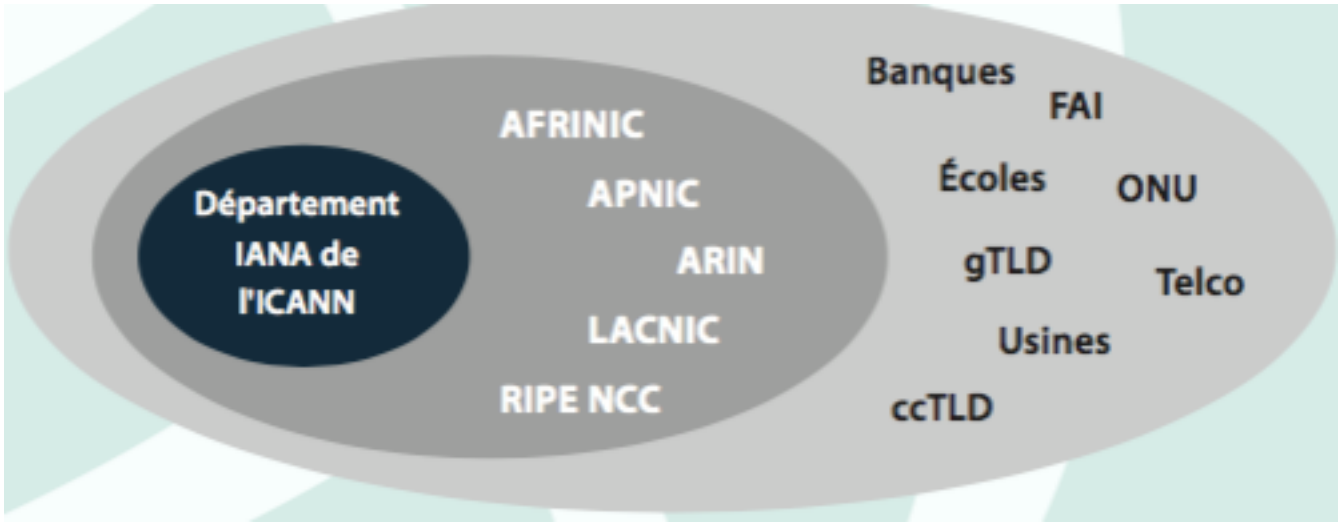
Le DNS (système de noms de Domaine)

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.

- Deux types de noms de domaines de premier niveau: génériques et codes pays
- Besoin de sécuriser le DNS pour un bon fonctionnement de l'Internet


Transition IPv4 – IPv6

Distribution des adresses IP



Distribution des adresses IP

AFRINIC (African Network Information Center) est le régistre régional de l'ICANN pour l'AFRIQUE.

AFRINIC s'occupe de la gestion et de l'attribution des resources internet telles que les adresses IP et les Numéros de système Autonome (ASN) pour l'Afrique.

AFRINIC a quelques programmes visant à promouvoir un rapide déployement du protocole IPv6 dans les réseaux an Afrique. www.afrinic.net

Les adresses IPv4

- Le déploiement de la version 4 du protocole a démarré en Janvier 1983 et est encore largement utilisée.

- Les adresses IPv4 sont des adresses de 32-bits écrites sous la forme de 4 octets (en décimale).

Par exemple: 192.0.2.53

On distingue les addresses privées et les adresses publiques.
IPv4 permet un nombre d'adresses limité à 4 294 967 296

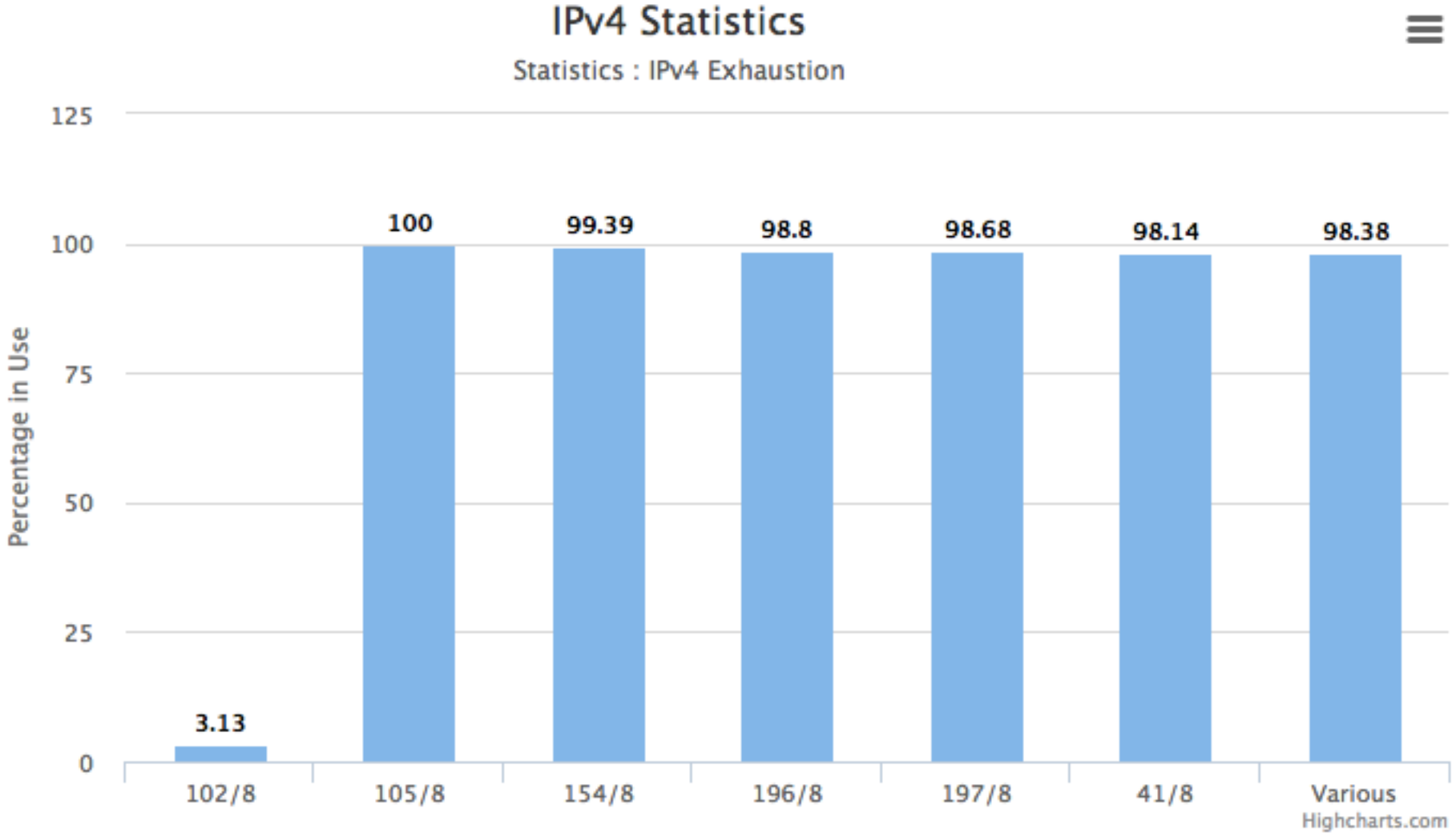
Les adresses IPv6

- Le déploiement d'IPv6 a commencé en 1999. Les adresses IPv6 ont une longueur de 128 bits et s'écrivent en hexadécimale. Exemple: 2001:0db8:582:ae33::29
- On peut disposer de 340 282 366 920 938 463 463 374 607 431 768 211 456 adresses IPv6 !
- En théorie, il existe 667 132 000 milliards d'adresses IPv6 possibles par millimètres carrés de surface terrestre.
- Selon les estimations, nous devrions en pratique être capable de disposer d'au minimum 1564 adresses IP par mètre carré de surface terrestre (océan compris).

Epuisement des adresses IPv4 – Deployer IPv6

- Un nombre de plus croissant d'utilisateurs de l'Internet
- L'un des taux de pénétration les plus élévés en Afrique
- De plus en plus d'équipements connectés
- Un plus grand besoin d'adresses IP
- AFRINIC n'a donc qu'un dernier bloc d'adresse IPv4 à allouer
- Nécessité donc d'aller vers IPv6

Sur le dernier bloc d'AFRINIC



Mécanismes de transition Ipv4-IPv6

- Techniques Dual Stack: IPv6 et IPv4 coexistent sur le même noeud
- Techniques de Tunnel: Pour éviter des dépendances dans le déploiement
- Techniques de translation: Permettre à des hôtes IPv6 pur de communiquer avec des hôtes IPv4 pur

Avoir un plan de transition

- Sensibilisation
- Renforcement de capacité
- Contrôle de compatibibilé
- Stratégie Nationale


Sécurité du DNS - Roulement de la clé KSK de la Zone Racine

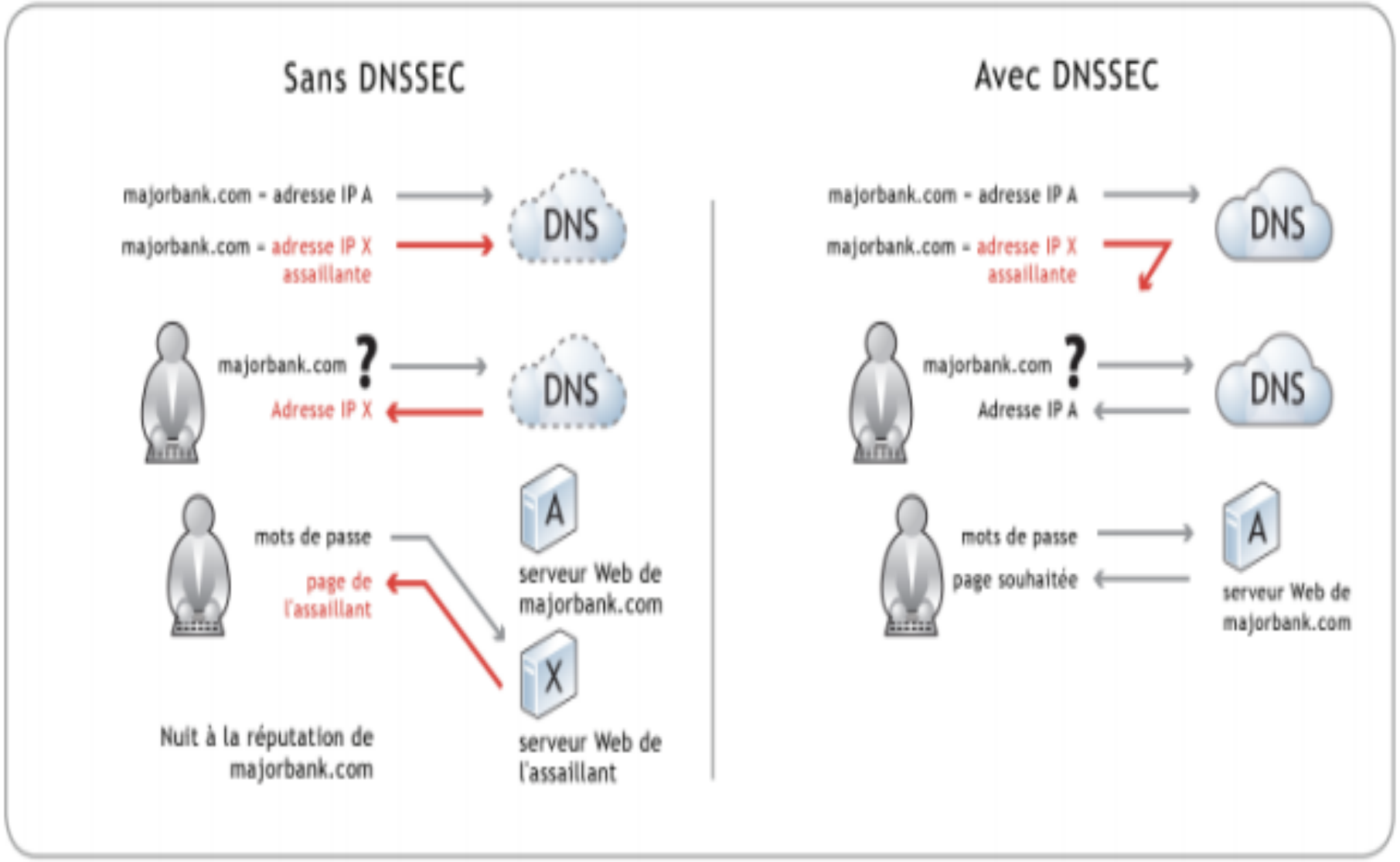
Le protocole DNSSEC

DNSSEC est l'abréviation de "DNS Security Extensions” (extensions de sécurité du DNS). DNSSEC ajoute un niveau de sécurité au DNS en incorporant une cryptographie de clé publique dans la hiérarchie du DNS, ce qui donne une seule infrastructure de clé publique (Public Key Infrastructure ou PKI), ouverte et mondiale pour les noms de domaine.
Aujourd’hui nous avons seulement 14 pays africains ou le DNSSEC est mis en oeuvre au niveau des ccTLDs.

Empoisonnement du Cache DNS

L'**empoisonnement du cache DNS** ou **pollution de cache DNS** (*DNS cache poisoning* ou *DNS cache pollution* en anglais) est une technique permettant de leurrer les serveurs DNS afin de leur faire croire qu'ils reçoivent une réponse valide à une requête qu'ils effectuent, alors qu'elle est frauduleuse. Une fois que le serveur DNS a été empoisonné, l'information est mise dans un cache, rendant ainsi vulnérables tous les utilisateurs de ce serveur. Ce type d'attaque permet, par exemple, d'envoyer un utilisateur vers un faux site dont le contenu peut servir à de l'hameçonnage (technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité).

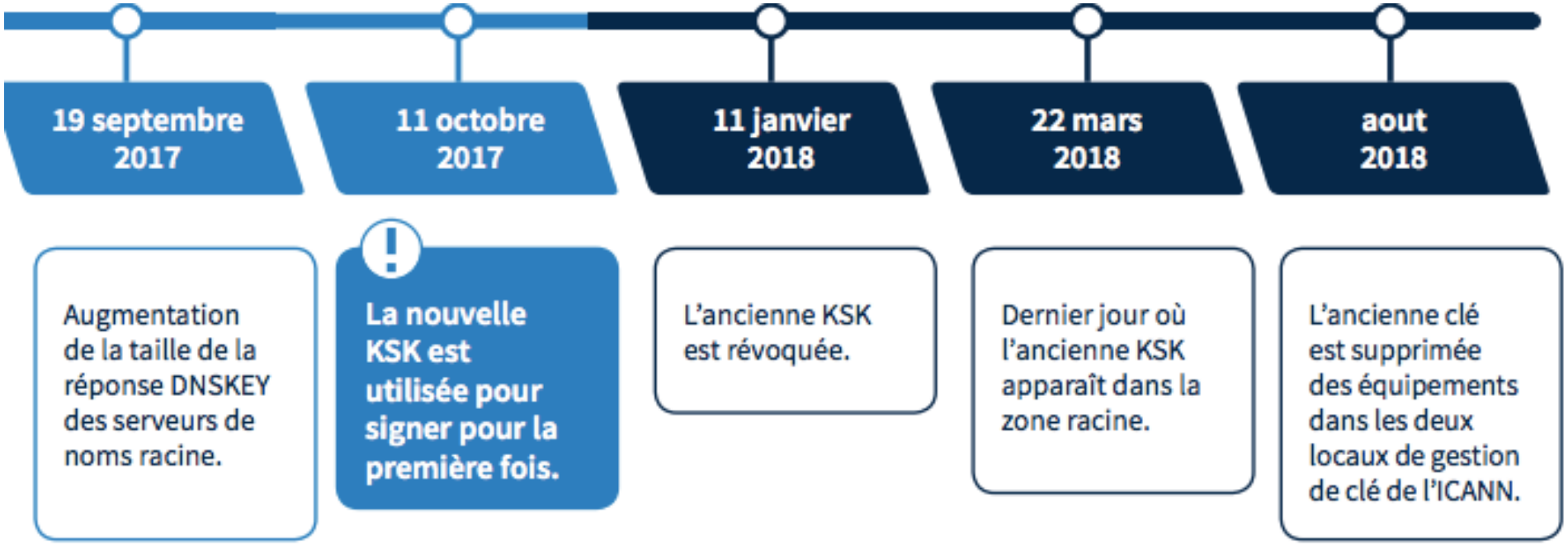
Illustration du DNSSEC



La KSK et Pourquoi la rouler?

- Il y a une paire de clés cryptographiques publique-privée utilisée pour le DNSSEC
- Question de politique comme pour un mot de passe
- DNSSEC mis en oeuvre en 2010
- Roulement prévu après 5 ans de fonctionnement

Calendrier



Préparer vos systèmes pour le roulement de la KSK de la racine

https://youtu.be/Lph39UgS7e4

Que Faire

Si votre logiciel permet les mises à jour automatisées des ancres de confiance du DNSSEC(RFC 5011) :

La KSK sera mise à jour automatiquement au moment approprié. Vous ne devez prendre aucune mesure supplémentaire.

Il convient de noter que 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.

À partir du 17 mars 2017, l'ICANN propose une plateforme d'essai pour les opérateurs de réseau et autres parties souhaitant s'assurer que leurs systèmes peuvent gérer correctement le processus de mise à jour automatique. Pour plus d'informations, consultez **icann.org/kskroll.**

CONCLUSION

- Du fait que Les adresses IP sont nécessaires pour le DNS et de l'épuisement de IPv4, il est est donc important de se préparer en vue d'une bonne transition vers Ipv6.
- Les régulateurs s devraient s'intéresser aux processus de développement des politiques au niveau des Registres Internet Régionaux.
- Pour le roulement de la KSK, il est aussi important de savoir ce que font les FAI et les sensibiliser.

Impliquez-vous et informez-vous

Participez à une réunion publique de l'ICANN. Trois fois par an, l'ICANN tient des réunions publiques et ouvertes dans différentes régions du monde. Pour en savoir plus, rendez-vous sur **meetings.icann.org**.

Rendez vous sur **go.icann.org/journey** pour savoir comment participer à une réunion publique de l'ICANN dans le cadre du programme NextGen@ICANN ou du programme de bourses de l'ICANN.

Suivez un cours en ligne gratuit à **learn-fr.icann.org**.

Participez à des événements dans votre région.

Allez sur **icann.org/community** pour trouver et rejoindre un groupe de la communauté de l'ICANN.

Inscrivez-vous pour recevoir les actualités et les bulletins régionaux de l'ICANN.

Suivez l'ICANN sur les médias sociaux

- @icann
- @icann_fr
- facebook.com/icannorg
- linkedin.com/company/icann
- youtube.com/ICANNnews
- flickr.com/icann
- soundcloud.com/icann
- slideshare.net/icannpresentations