Comprendre le DNS (système des noms de domaine) - DNSSEC

Yaovi Atohoun

FFGI2019

26-30 Août 2019; Ouagadougou – Burkina Faso

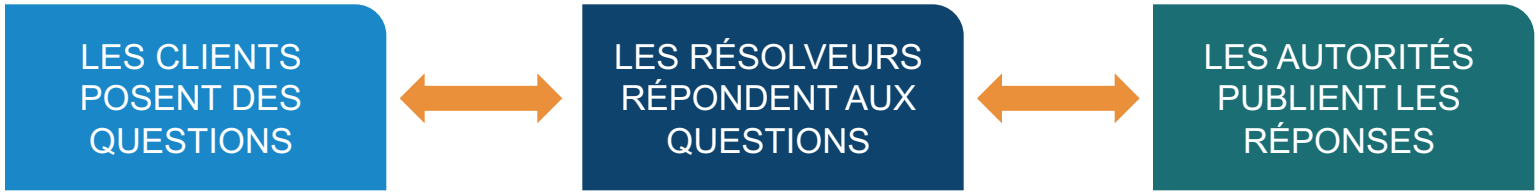
ICANN

Les Identifiants de l'Internet

- L'internet est un réseau maillé dont les opérateurs acceptent de communiquer à travers des protocoles prédefinis (TCP/IP)

- Les réseaux utilisent des identifiants pour nommer ou numéroter des ordinateurs individuels (hôtes) de sorte à ce qu'ils communiquent entre eux:
  - Les adresses IP identifient les rues et les numéros de maison
  - Les numéros de system Autonomes (ASN) identifient un "quartier" Internet
  - Le nom de domaine est le moyen pratique pour se rappeler d'une adresse

Éléments du DNS vulnérables aux attaques



- **Les serveurs de noms faisant autorité** hébergent les données de zone, c'est à dire, l'ensemble des données DNS publiées par les titulaires de noms de domaine.
- **Les résolveurs de noms récursifs** (résolveurs) sont des systèmes qui permettent de trouver des réponses à des requêtes pour des données du DNS.
- **Les résolveurs de mise en cache** trouvent et gardent les réponses au niveau local pendant un certain temps dit temps de validité de la réponse (TTL).
- **Les résolveurs client ou basiques** sont les logiciels des applications, des applications mobiles ou des systèmes d'exploitation qui interrogent le DNS et traitent les réponses.

C’est quoi le “Système de Nom de Domaine” (DNS)

- Une base de donnée distribuée principalement utilisée pour obtenir une adresse numérique IP.

  Ex: 192.168.23.1 ou fe80::226:bbff:fe11:5b32 associée a un nome mnemonique www.example.com

- Pourquoi avons nous besoins du DNS?
  - Il est difficile de retenir une succession de nombre décimaux
  - il est pratiquement impossible de long nombres hexadécimaux

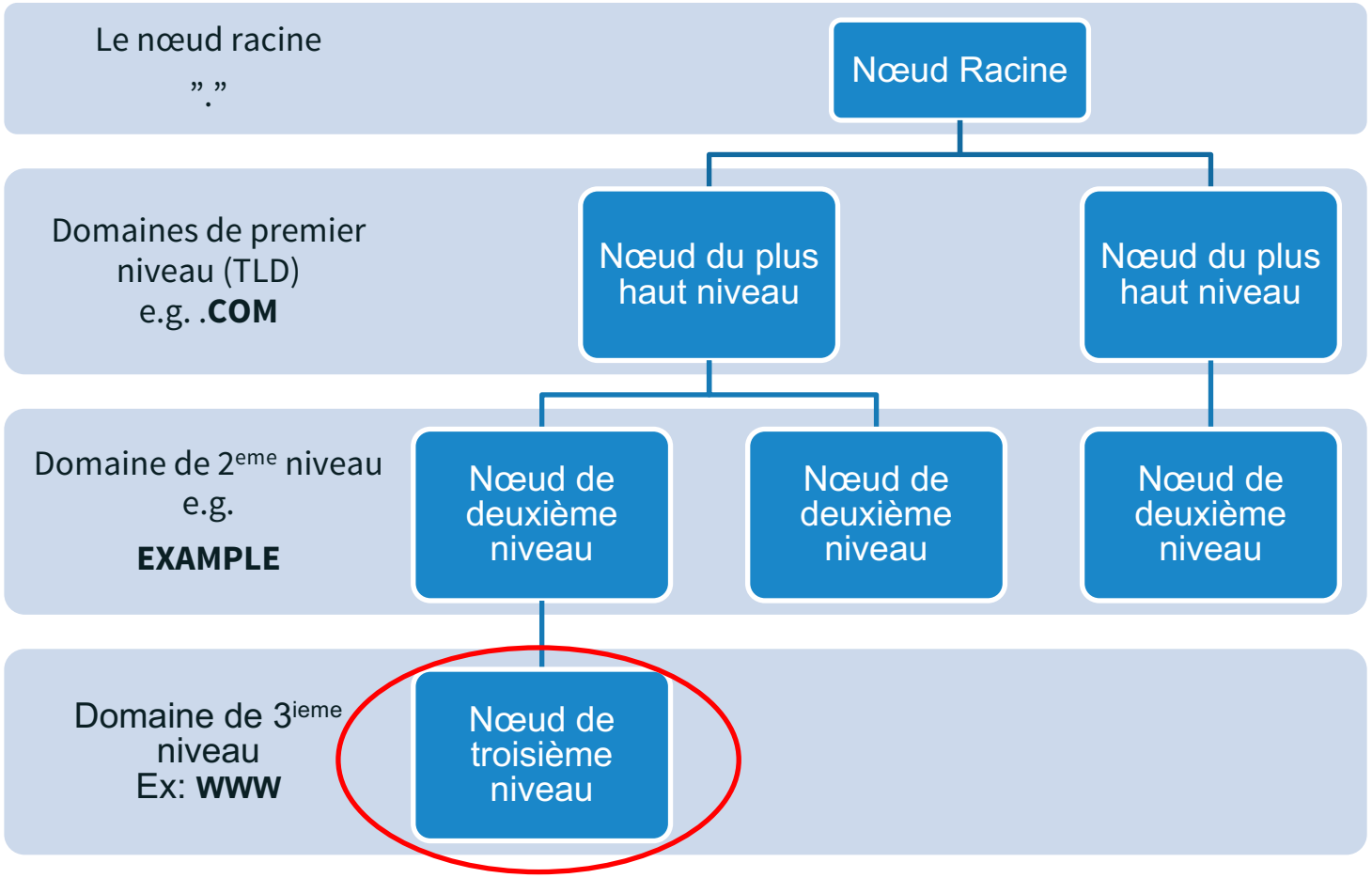
Le DNS est un Service d'Annuaire Public

- Service a travers lequel les Entreprises et les individus publient les noms et les adresses de leur présence en ligne.

- Caractéristiques fondamentales des informations dans le DNS.
  - Vous ne pouvez pas appliquer des lois de copyright: Elles sont faites pour être copiée.
  - Si vous les gardez confidentiellement, personne ne pourra vous trouver
  - Les données du DNS sont généralement temporelles
    - Les noms sont enregistrés/assignés et pas des propriétés
    - Les adresses IP sont allouées ou assignées et pas des propriétés
    - Les donnés du DNS et même certaines adresses IP ont une durée de vie limitée.
  - Vous ne pourrez empêcher personne de les collecter

Labels et Nom de Domaines

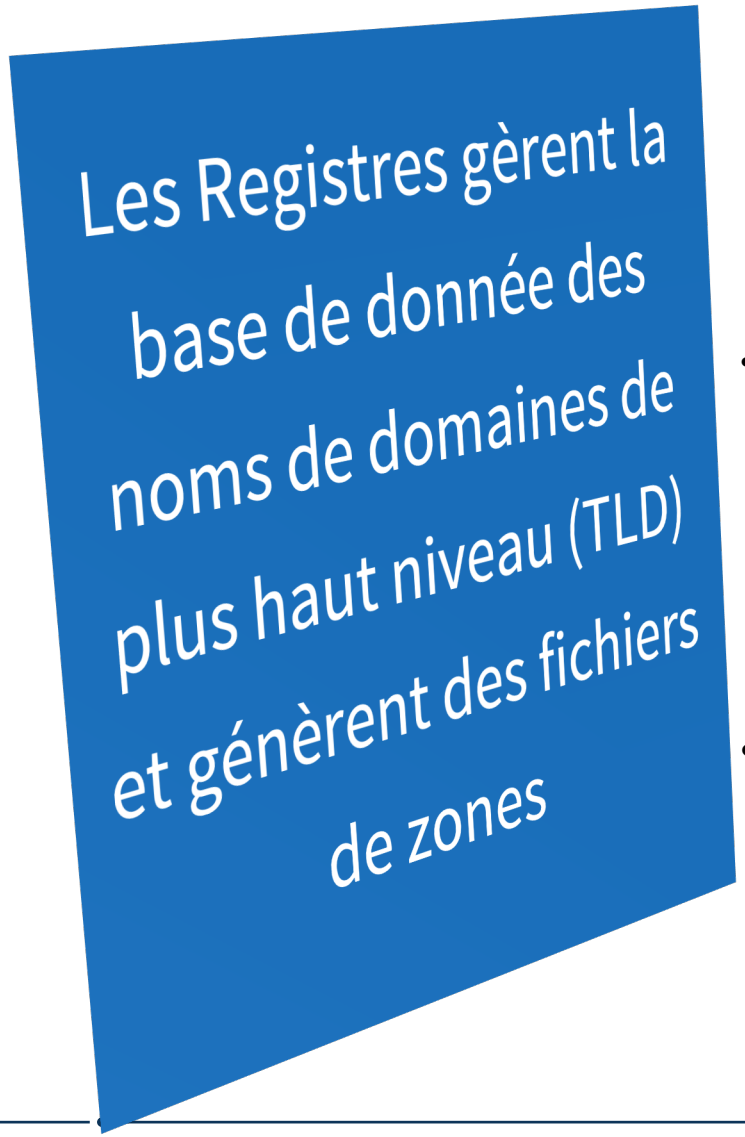
Chaque nœud dans l'espace DNS a un label.
Le nom de domaine d'un nœud est la liste des labels en parcourant la chaine du nœud à nommé vers la racine du DNS



Le nom de domain du noeud encerclé en rouge est **www.example.com.**

Ceci s'appel
NOM DE DOMAINE COMPLETEMENT QUALIFIE
(ou FULLY QUALIFIED DOMAIN NAME (FQDN))
Les FQDN sont globalement unique dans l'espace public DNS

Qui fait quoi dans l'écosysteme du DNS?



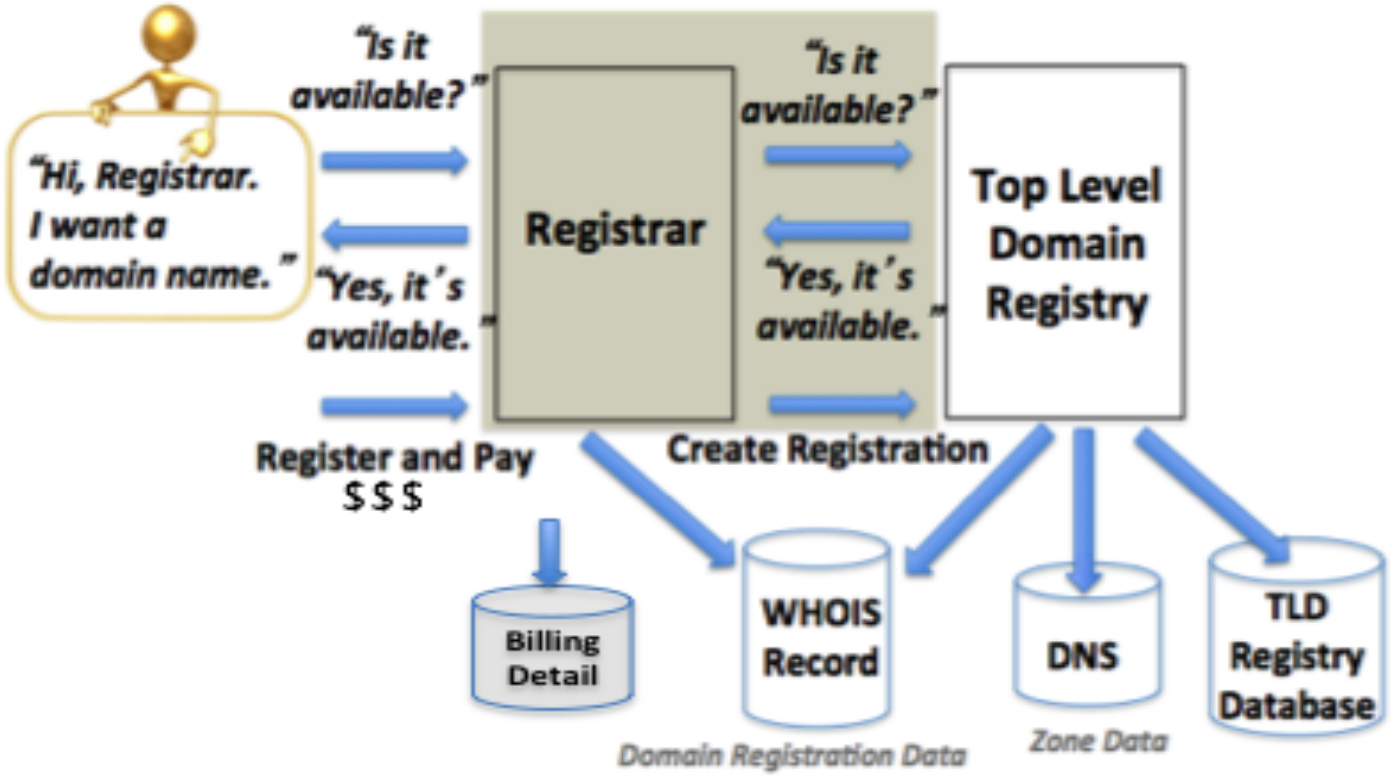
- Les Operateurs de gTLD sont contracteurs d'ICANN
  - Doivent adhérer aux règles (consensuelles) définies par la communauté
  - La liste des registres accrédités est consultable à: http://www.icann.org/en/resources/registries/listing
- Les Operateurs de ccTLD n'ont pas de contrat avec ICANN
  - Peuvent sous-traiter leur service d'enregistrement ou de WHOIS à des Opérateurs de gTLD.
  - Ils contribuent aux travaux de la communauté ICANN a travers le ccNSO - http://ccnso.icann.org
- Les Operateurs de Registres peuvent être:
  - De larges entreprises,
  - Des organisation à but (non-)lucratif
  - Des départements Universitaires
  - Des Agences gouvernementales
  - Entièrement opérés par des tierces parties contractante

Les Régistrars

- Dans le contexte des gTLDs, tous les régistars doivent être accrédités par ICANN et sujets au "Registrar Accreditation Agreement (RAA)"
- Les ccTLD eux définissent leur propre processus d'enregistrement de noms.
- Les revendeurs (détaillants ou grossistes)
- L'enregistrement de noms n'est pas une activité commerciale exclusive
  - Ils peuvent être combinés avec l'hébergement Web, DNS, mail, ou autre services de transaction marchande en ligne

https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en
http://www.icann.org/registrar-reports/accredited-list.html

Processus de base pour l'enregistrement d'un nom de domaine



Comment enregistrer un nom de domaine générique (gTLD):

1. Choisir un mot ex: exemple
2. Visiter le régistrar pour vérifier la disponibilité du mot dans le TLD
3. Payer les frais pour enregistrer le nom de domaine.
4. Soumettre les informations d'enregistrement

Les registres et les Régistrars gèrent:

- "mot" + TLD (exemple.info) (géré dans la BD du Registre)
- Contactes & DNS (géré dans le Whois)
- DNS, statut (géré dans la base de donne WHOIS)
- Les informations de payement

Composantes opérationels du DNS

- Les nom de serveurs Autoritatifs hébergent les données de zone
  - L'ensemble de “Données DNS” que l’enregistreur (Registrant) publie.
- Résolveur de nom Récursif (“resolvers”)
  - Le systèmes qui trouve des réponses aux requêtes de données DNS
  - Les résolveurs Cache quand à eux trouvent et enregistrent les réponses localement pour une période “TTL” (Time To Leave) donnée.
- Résolveurs Client ou “stub”
  - Logiciels dans les application, app mobiles ou système Opérationnels qui envoient les requêtes DNS et traitent les réponses.

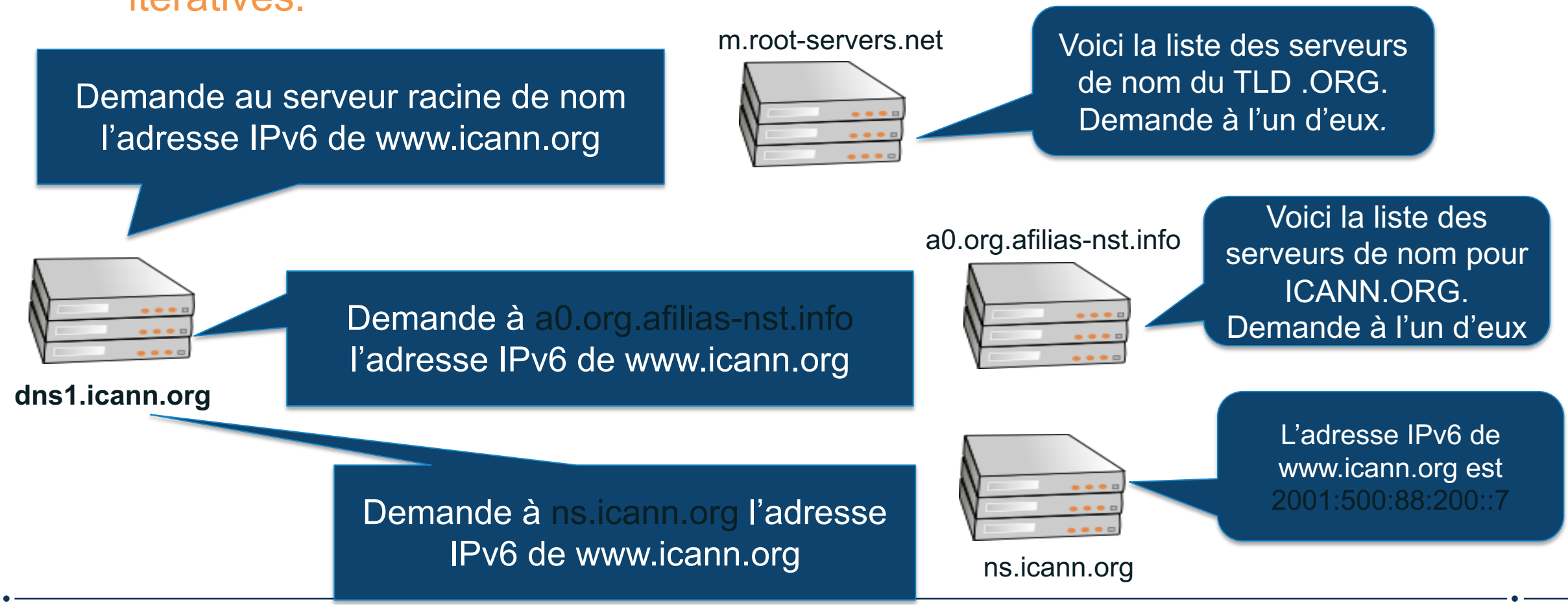
DNS: Système d'assistance du répertoire Internet

- Les Résolveurs Stub posent les questions
  - Généralement sous forme de logiciel dans les applications, app mobiles ou système Opérationnels aui envoie les requêtes DNS et traite les réponses
- Les résolveurs de nom Récursifs trouvent les réponses aux requêtes de données DNS.

Récursion (aussi connu sous le nom de résolution itérative)

Comment un résolveur arrive-t-il à trouver l'adresse de WWW.ICANN.ORG?

- Les Résolveurs trouvent des réponses en posant eux même des questions itératives.



Données de zone DNS

- Les données de Zone DNS sont hébergées sur un serveur de nom autoritatif
- Chaque type de domaine à des données de zone (racine, TLD, délégations)
- La Zones contient des enregistrements ressource (*Resource Records - RR) qui décrivent*
  - Les serveurs de noms,
  - les adresses IP,
  - Les hôtes (du domaines),
  - Les Services
  - Les clés Cryptographiques keys & signatures…

Seulement les caractères US ASCII-7, nombres, et trait d'unions peuvent être utilisés dans des données de zone. Dans une zone, les chaines de caractère IDNs débutent avec XN--

Pourquoi le DNS est-il la cible d’attaques ?

- Le DNS assure la traduction des noms de domaine en adresses IP (protocole Internet).
- Toute perturbation du DNS entraîne la perturbation des transactions commerciales, des services gouvernementaux, de l’apprentissage en ligne ou de l’interaction sociale.
- L’exploitation du DNS permet à l’attaquant de tromper les utilisateurs.
- Vecteurs d’exploitation :
  - Enregistrement malveillant de noms de domaine.
  - Détournement de la résolution de noms ou des services d’enregistrement.
  - Altération des données du DNS.

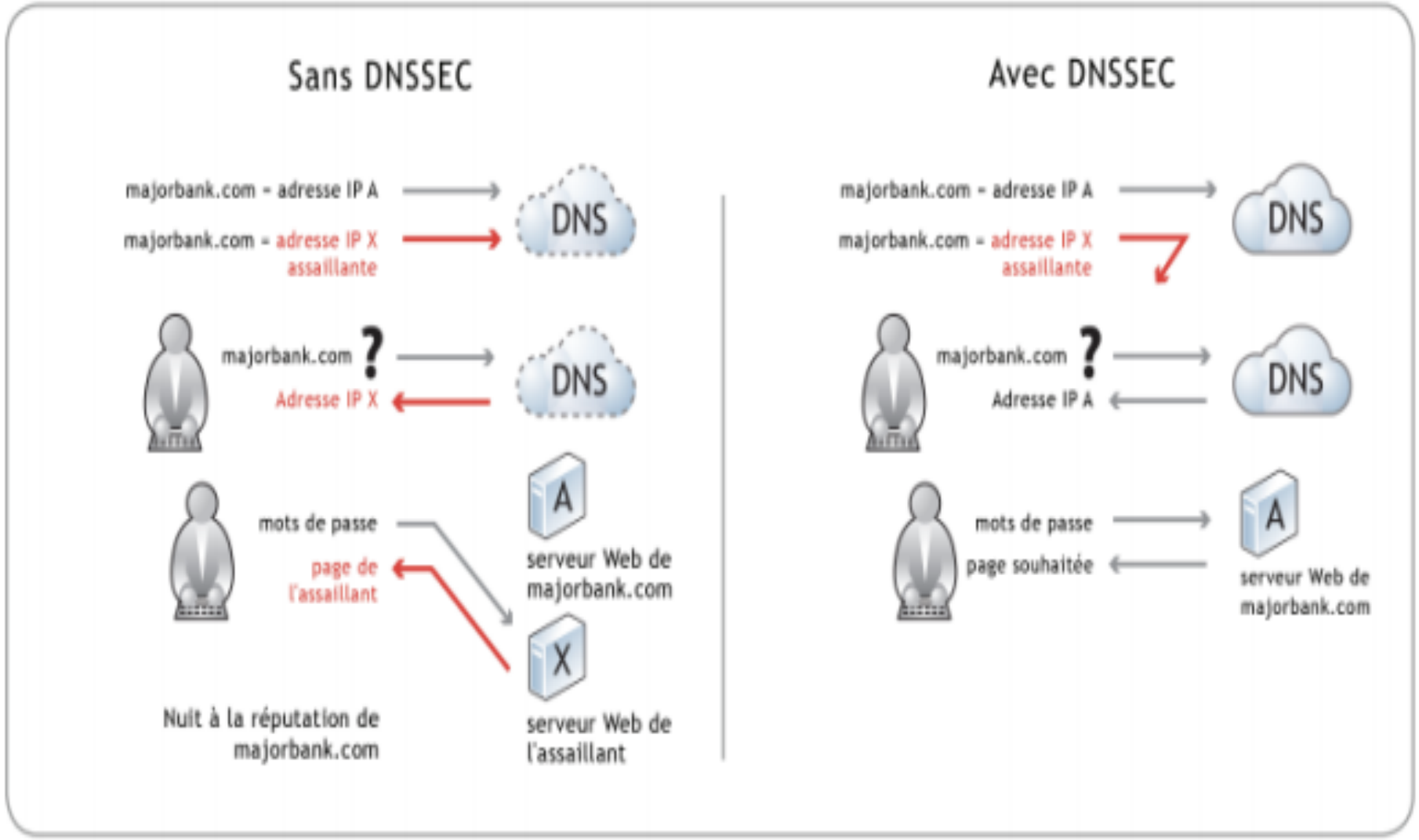
DNSSEC

C’est quoi le DNSSEC ?

Le DNSSEC sont les **extensions de sécurité du système des noms de domaine (DNS).**

- Il s’agit d’un protocole déployé pour sécuriser le DNS.
- Le DNSSEC sécurisent le DNS en incorporant la cryptographie à clé publique dans la hiérarchie du DNS, ce qui résulte en une infrastructure unique et ouverte de gestion de clés publiques (PKI) pour les noms de domaine.
- Les DNSSEC sont le fruit de dix ans de travail communautaire pour le développement de normes ouvertes.

Illustration du DNSSEC



Le projet DNSSEC Roadshow

- Mise en Œuvre dans la stratégie africaine
- Manifestation d'un hôte au niveau du pays
- Atelier de trois
  - Jour #1 : journée d'information pour tous les acteurs
  - Jour #2 : journée de formation technique
  - Jour #3 : élaboration de plan de mise en œuvre avec l'équipe du ccTLD

Plus d'information et de ressources sur le site http://dnssec-africa.org

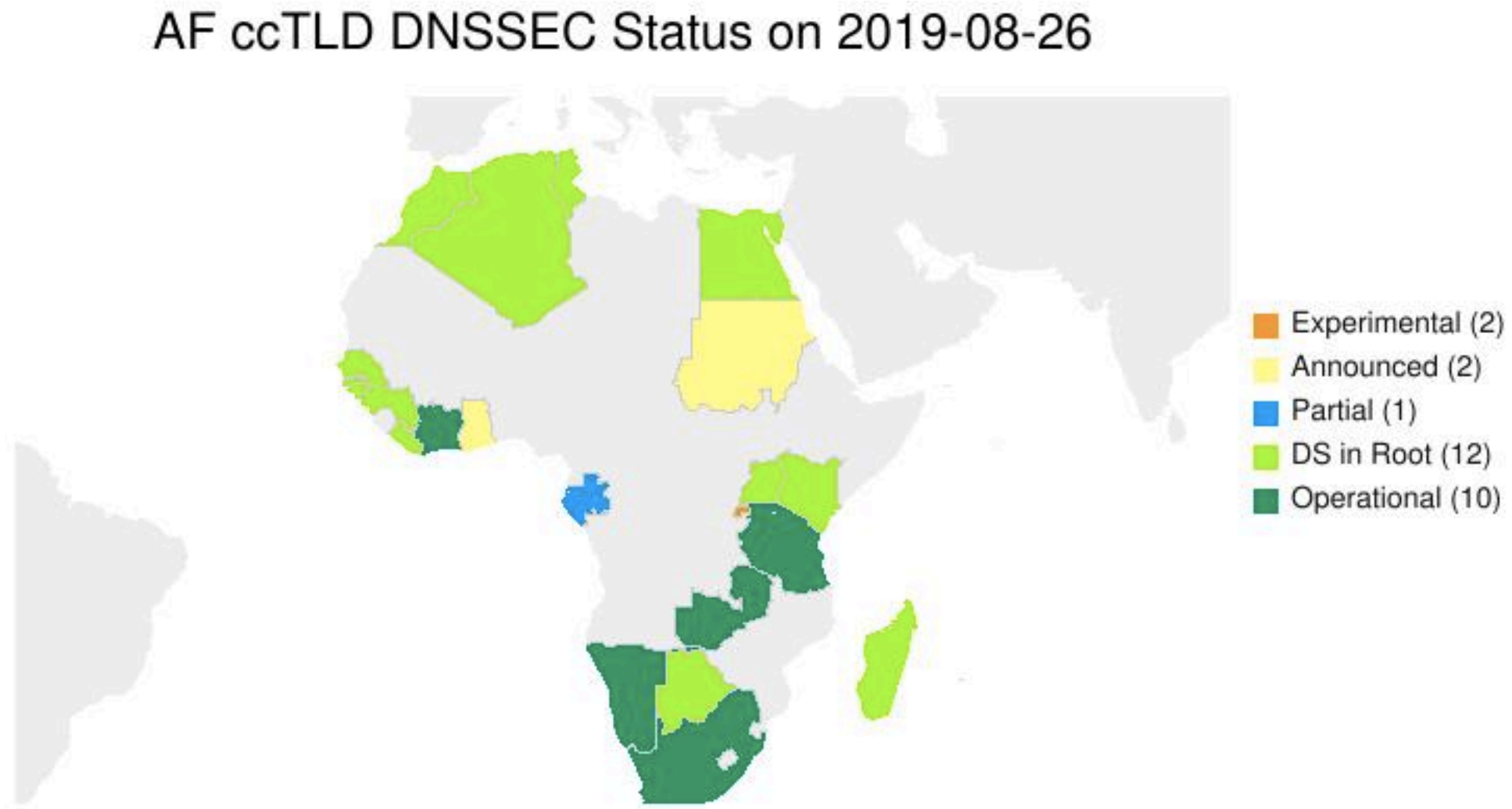
Le Projet DNSSEC Roadshow de la stratégie africaine

TLD	Date de la tournée	Pays	Statut	DNSKEY	Date de l'enregistrement DS
.km	13-15 septembre 2017	Comores	Non signé		
.td	17-19 janvier 2017	Tchad	Non signé		
.bj	24-26 août 2016	Bénin	Non signé		
.gh	22-24 mars 2016	Ghana	Non signé		
.ma	29 février - 2 mars 2016	Maroc	Signé	21/02/2014	20/02/2016
.tg	17-19 février 2016	Togo	Non signé		
.za	8-10 juillet 2015	Afrique du Sud	Signé	09/12/2016	17/12/2016
.mg	4-6 mai 2015	Madagascar	Signé	17/03/2016	19/03/2016
.cg	11-13 mars 2015	Congo	Non signé		

Le Projet DNSSEC Roadshow de la stratégie africaine

.ci	25-27 février 2015	Côte d'Ivoire	Non signé		
.bw	1-3 décembre 2014	Botswana	Signé	22/11/2015	04/12/2015
.cm	17-19 septembre 2014	Cameroun	Non signé		
.bf	19-21 mai 2014	Burkina Faso	Non signé		
.zm	28-30 avril 2014	Zambie	Signé	03/10/2015	09/10/2015
.sn	19-21 mars 2014	Sénégal	Signé	01/09/2016	01/10/2016
.rw	10-12 mars 2014	Rwanda	Non signé		
.tz	18-20 septembre 2013	Tanzanie	Signé	13/10/2012	09/02/2013
.ng	26-27 juin 2013	Nigéria	Non signé		
.ke	11-13 juin 2013	Kénya	Signé	23/02/2014	21/03/2014

Autres sources d'information sur le DNSSEC



Source: http://www.internetsociety.org/deploy360/dnssec/maps/

Questions?

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann