DNSSEC C'EST QUOI ?

ET ON EN EST OU ?

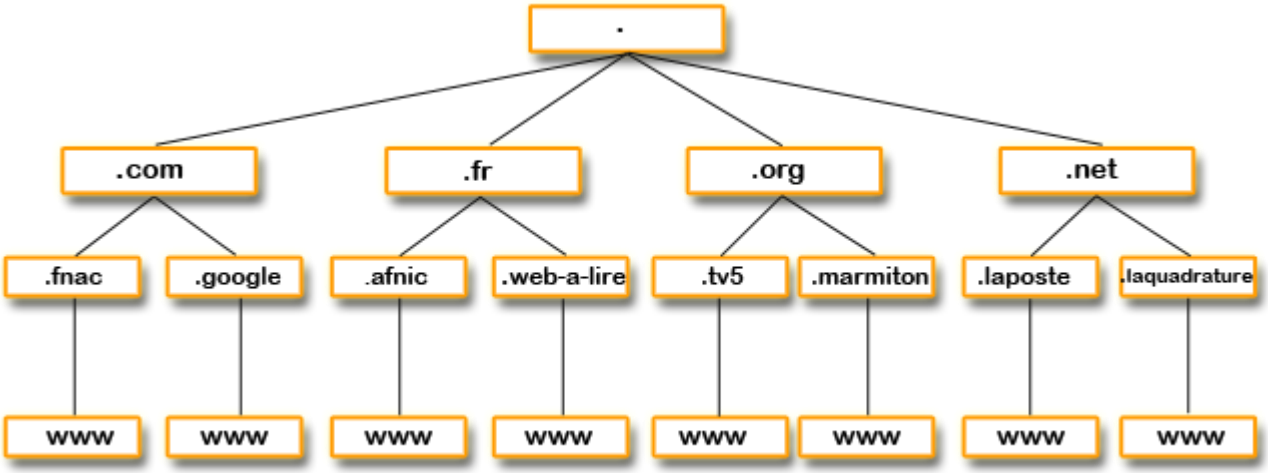
ESIPE – IR3
LATKOVIC Gérald

PLAN

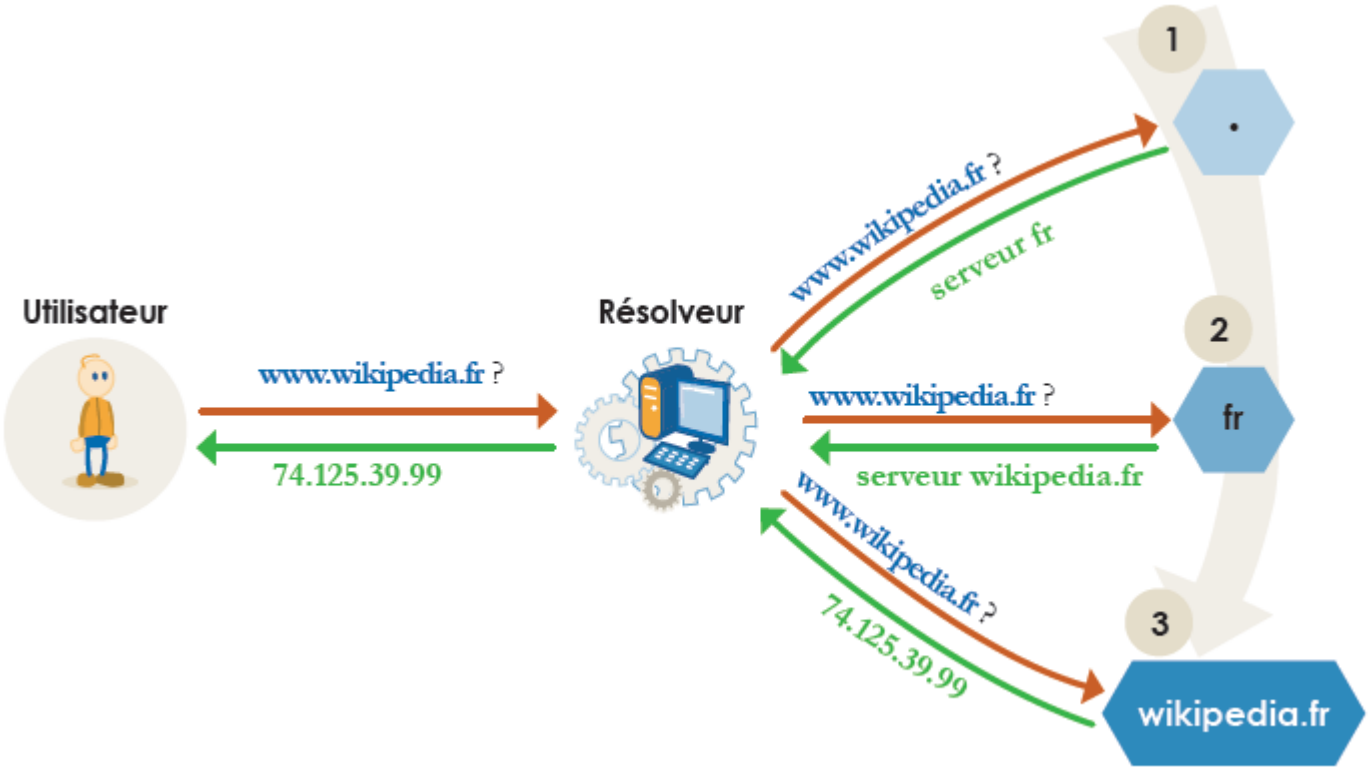
- Léger rappel de DNS
- Les vulnérabilités
- Problématique et enjeux
- DNSSEC
  - Fonctionnement
  - Le déploiement
  - Avoir son propre résolveur DNSSEC ?
  - Les alternatives
  - Conclusion

LÉGER RAPPEL DE DNS (1/2)

- Une brique fondamentale dans l'internet d'aujourd'hui
- Une base de données distribuée sur des millions de machines
- Défini et implémenté dans les années 80
- Fais la relation entre le nom d'une machine sur le web et une adresse IP

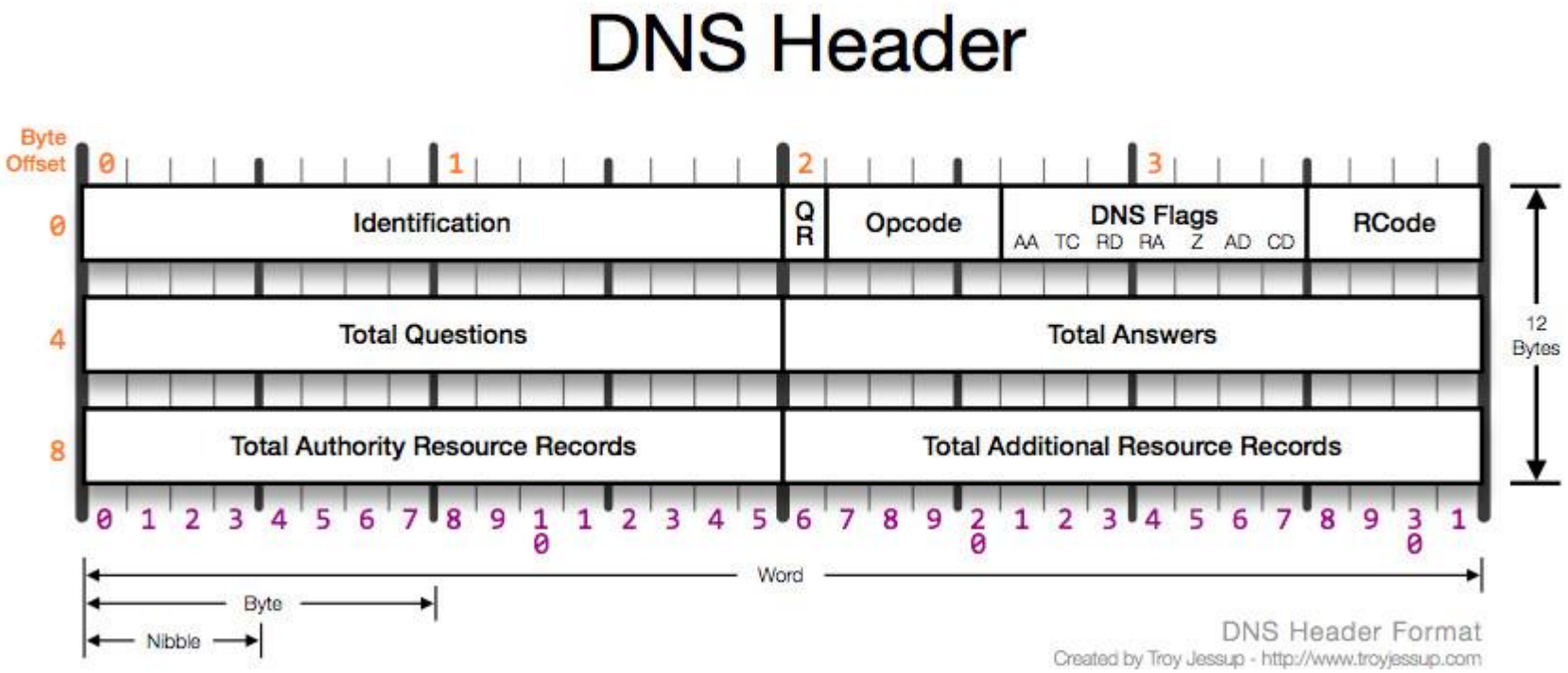


LÉGER RAPPEL DE DNS (2/3)



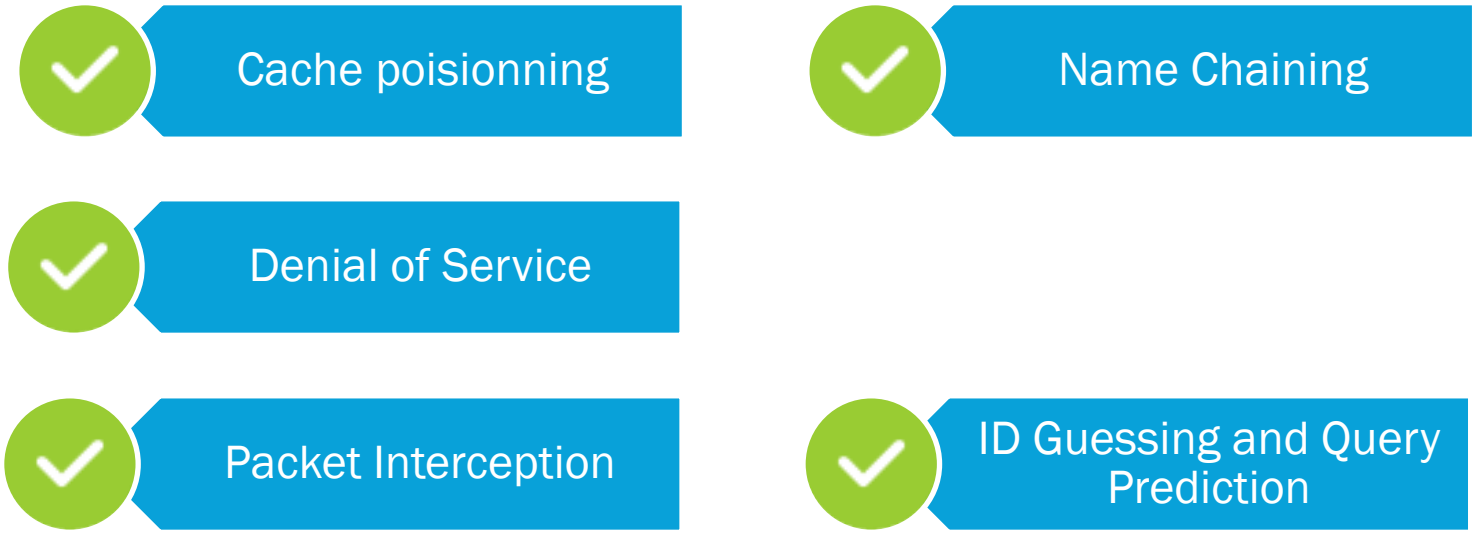
La résolution DNS (www.afnic.fr)

LÉGER RAPPEL DE DNS (3/3)



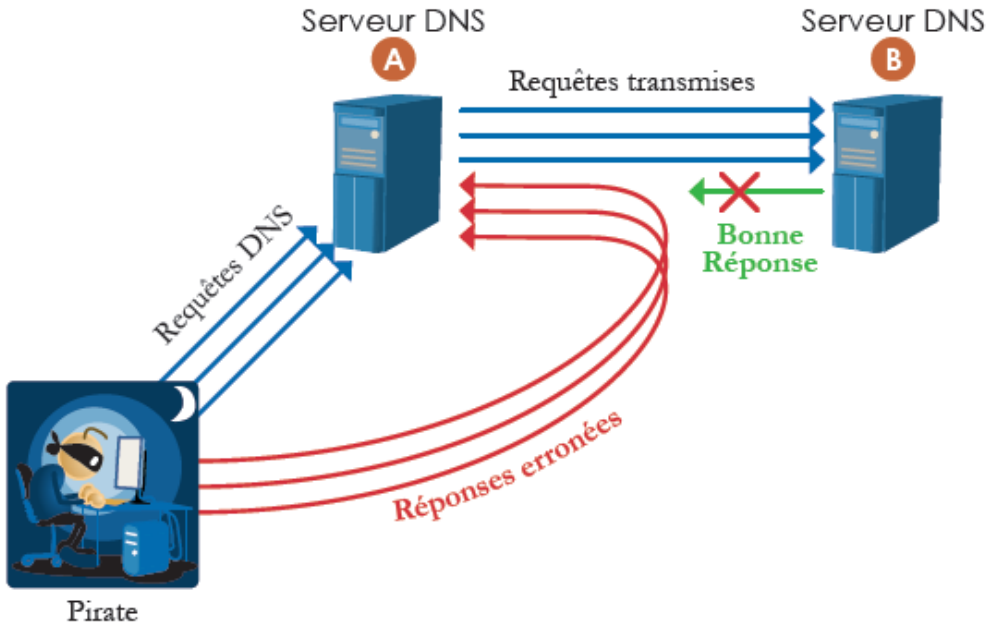
LES VULNÉRABILITÉS (1/2)

- DNS n'est pas sur (RFC 3833), les principaux problèmes connus sont :



LES VULNÉRABILITÉS (2/2)
EMPOISONNEMENT DE CACHE

- Faille Kaminsky (Black Hat 2008)
- Attaque de Bradesco à travers NET Virtua (ISP)



PROBLÉMATIQUE ET ENJEUX

- Comment assurer l'intégrité des données et authentifier les résolveurs / serveurs faisant autorité tout en conservant la rétrocompatibilité avec DNS ?

- Assurer la sécurité d'accès à la ressource demandée aux 3 milliards d'utilisateurs
- Trouver une solution assez légère pour ne pas surcharger les serveurs de noms

DNSSEC

Qu'est-ce que DNSSEC ?

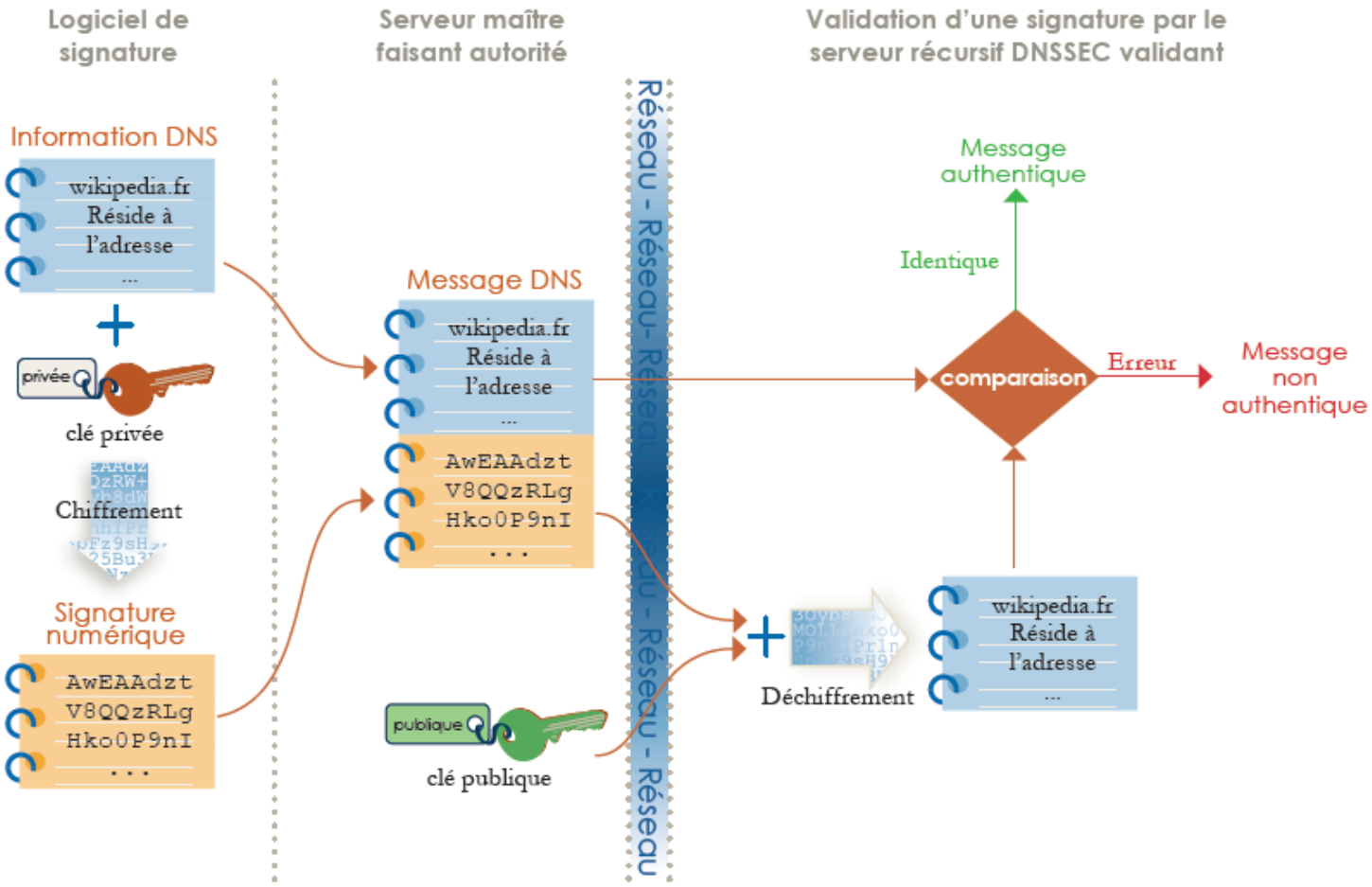
- Sécurisation des données (pas du canal) à travers un mécanisme de clés
- Signe les enregistrements DNS de sa propre zone
- Chaque zone DNS parente, garantie l'authenticité des clés de ses zones filles en les signant
- Permet d'établir une « chaine de confiance » jusqu'à la racine DNS

Ce que n'est pas DNSSEC

- Pas de chiffrement des enregistrements DNS
- Pas de confidentialité des échanges
- Ne garantit pas la sécurité d'un transaction (au sens certificat SSL)

DNSSEC – FONCTIONNEMENT

LE SYSTÈME DE CLÉS

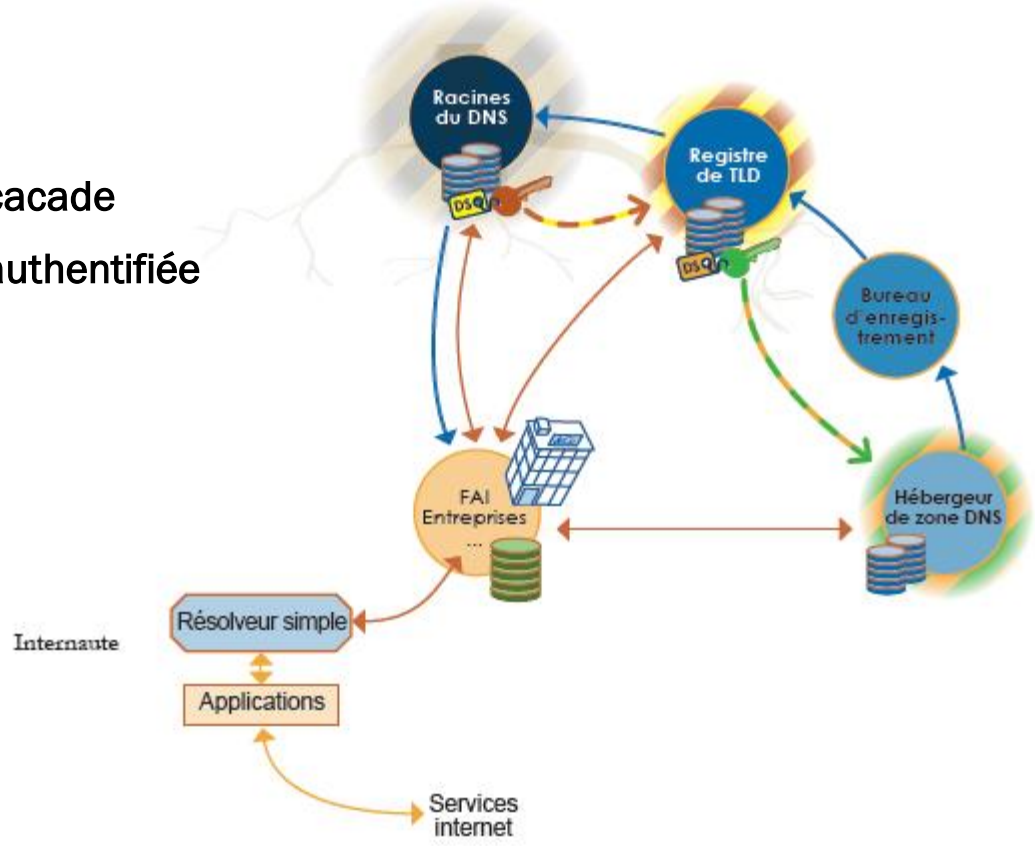


DNSSEC – FONCTIONNEMENT

LA CHAINE DE CONFIANCE

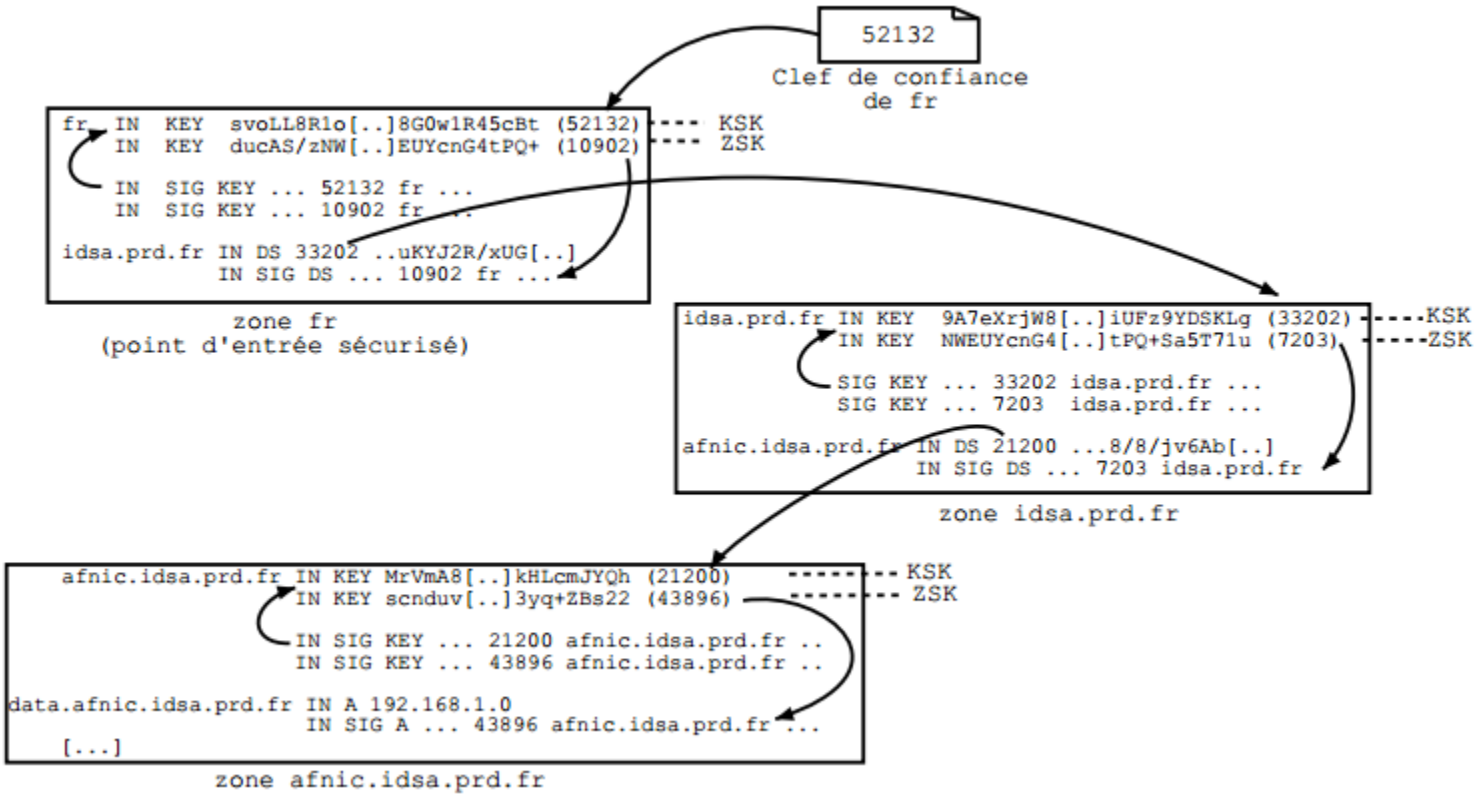
- Authentification de clés en cacade
- La clés d'une zone fille est authentifiée par celle de la zone parente

- Confiance récursive en aval

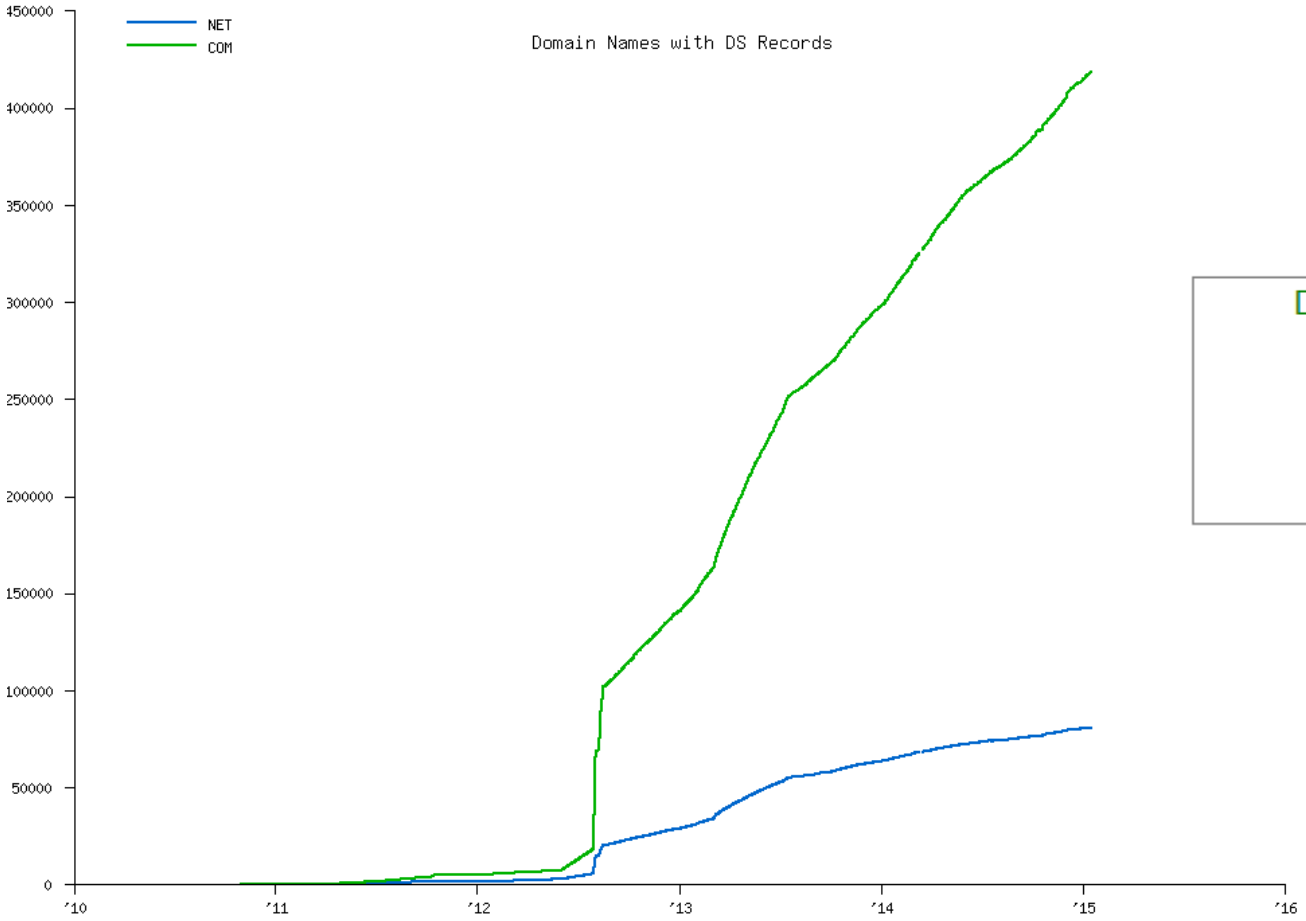


DNSSEC – FONCTIONNEMENT

LA CHAINE DE CONFIANCE



DNSSEC – LE DÉPLOIEMENT



VERISIGN

Domains Secured with DNSSEC

com	418,285
net	80,739
edu	67

Updated 2015-01-16 16:51:56

DNSSEC – LE DÉPLOIEMENT

- **Les RR de la zone racine ont étés signés en Juillet 2010**
  - (le .fr en Septembre 2010 !)

- **En France l'Afnic s'engage dans la promotion de DNSSEC :**
  - L'Afnic propose à ses bureaux d'enregistrement accrédités une remise de 20% sur le tarif des créations et la maintenances de noms de domaine en .fr signés par DNSSEC

- **Les « registrars » proposent le déploiement DNSSEC à leurs clients (nous !)**
  - OVH, Gandi (en maintenance) ..

DNSSEC

AVOIR SON PROPRE RÉSOLVEUR DNSSEC ?

- **Pourquoi ?**
  - Assurer son adhérence à la « chaine de confiance »
  - Contourner la censure réalisée par certains résolveurs (DNS RPZ)
  - On ne fait plus confiance aux DNS potentiellement fournis par DHCP (hotspots..)

- **A quel niveau ?**
  - Local
    - La « chaine de confiance » est complète car la validation DNSSEC est locale
    - On perd la notion de cache partagé => accroit la charge sur la racine
  - Distant
    - Possibilité de mutualiser le service
    - Partage de cache

DNSSEC

AVOIR SON PROPRE RÉSOLVEUR DNSSEC ?

- Unbound est un serveur DNS permettant de faire du DNSSEC (BIND aussi)
- Dans /var/unbound/etc/unbound.conf :

```
server:
    interface: 127.0.0.1
    auto-trust-anchor-file: "/var/lib/unbound/root.key"
```

- Récupération de la clé de la racine :
  - unbound-anchor -a "/var/lib/unbound/root.key"
- Dans /etc/resolvconf/resolv.conf.d/head :

```
nameserver 127.0.0.1
```

DNSSEC
LES ALTERNATIVES

- **DNSCurve : Sécurisation du canal (contrairement a DNSSEC)**
  - Inutile si le serveur distant est un serveur pirate

- **DNSCrypt : Chiffre aussi le trafic DNS (simple)**
  - Outil open source
  - Développé par OpenDNS

CONCLUSION

- DNSSEC protège contre des failles de type Kaminsky (cache poisoning)
- Il est en bonne voie de déploiement
- Il n'est pas simple à maintenir (rollover de clés)
- Repose sur la compétence des différents acteurs de la chaine de confiance

BIBLIOGRAPHIE

L'Afnic (www.afnic.fr)

Stephane Bortzmeyer, www.bortzmeyer.org (Afnic)

www.dnssec.net

RFC 3833

RFC 4033, 4034, 4035

VeriSign www.verisigninc.com/en_US/innovation/dnssec