Operations et Securité DNS

Maroc 24-26 Sept 2018

RIAHI Chamseddine NIC.tn

HISTORIQUE

- **Jusqu'en 1984 : réseau restreint militaire/universitaire/recherche**

  Hôtes de l' ARPAnet/Internet dans un fichier host.txt
  Mis à jour et diffusé par le SRI-NIC

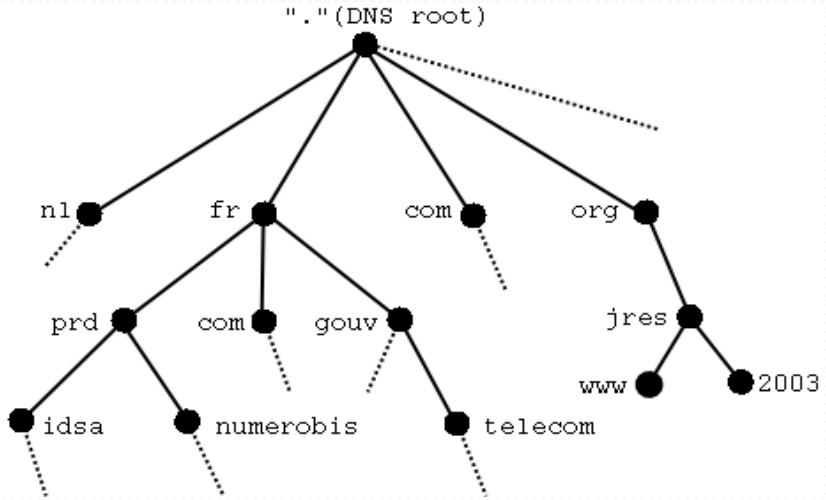
- **A partir de 1984 : croissance importante du nombre d'hôtes connectés**

  Un système de nommage distribué: le DNS
  RFC 1034/1035 (Paul Mockapetris)

- **1995 : généralisation du réseau et multiplication des usages**
  Le DNS : un principale protocole pour fonctionnement de l'Internet
  Besoin de sécurité
  1999: Extensions de sécurité au protocole DNS: DNSsec (RFC 2535)
- **2003 :**
  Premières expérimentations en cours
  Réécriture du protocole DNSsec en cours (Groupe de travail DNSext à l 'IETF)

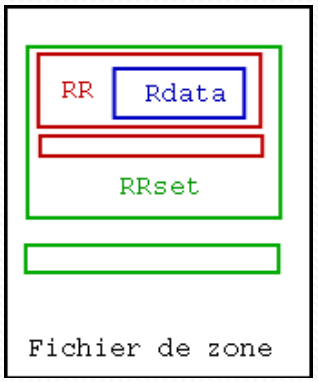
Modèle DNS

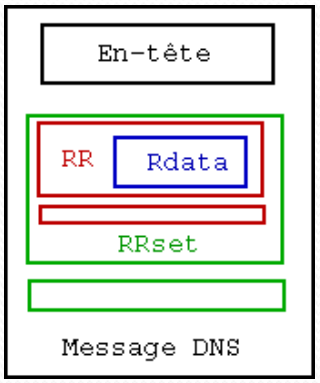
- Architecture client/serveur
- La base de données DNS contient les associations entre les noms de domaine et un certain nombre d'informations (adresses IP, relais mail, serveurs de nom, etc)
- Hiérarchique
- Distribuée
- Redondante



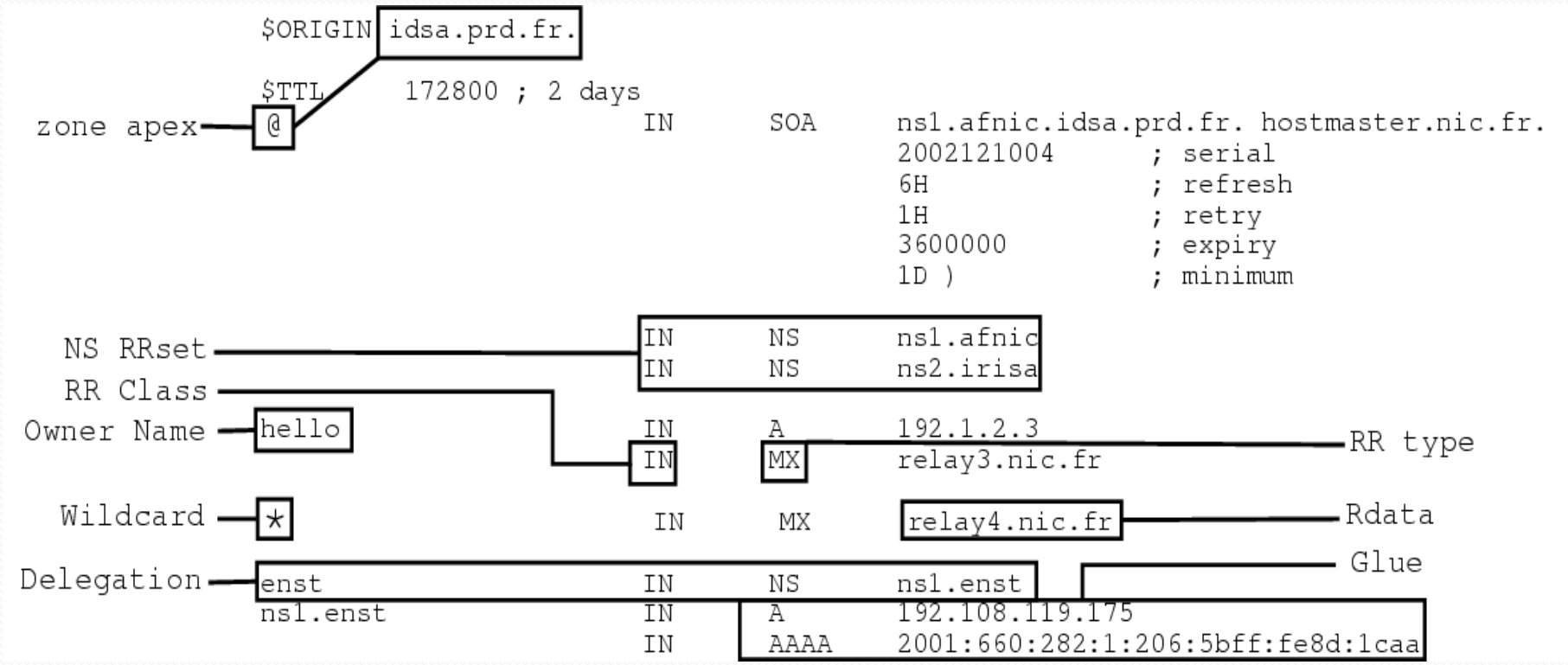
Elément du DNS

- Les enregistrements DNS (Resource Records: RRs)
- Les RRsets (les RRs de même type)
- Les fichiers de zone
- Les messages DNS (questions/Reponses)

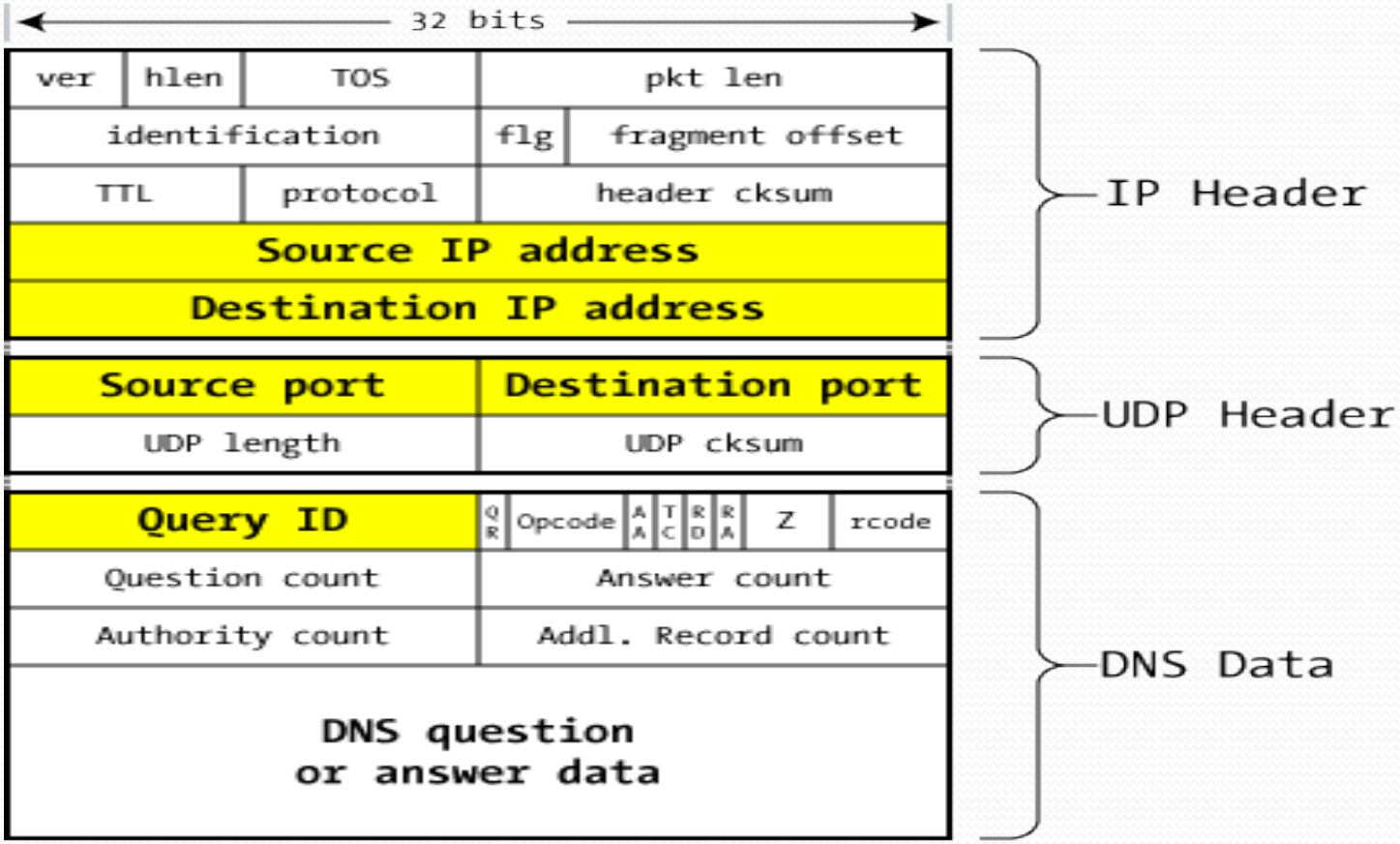




Fichier de zone

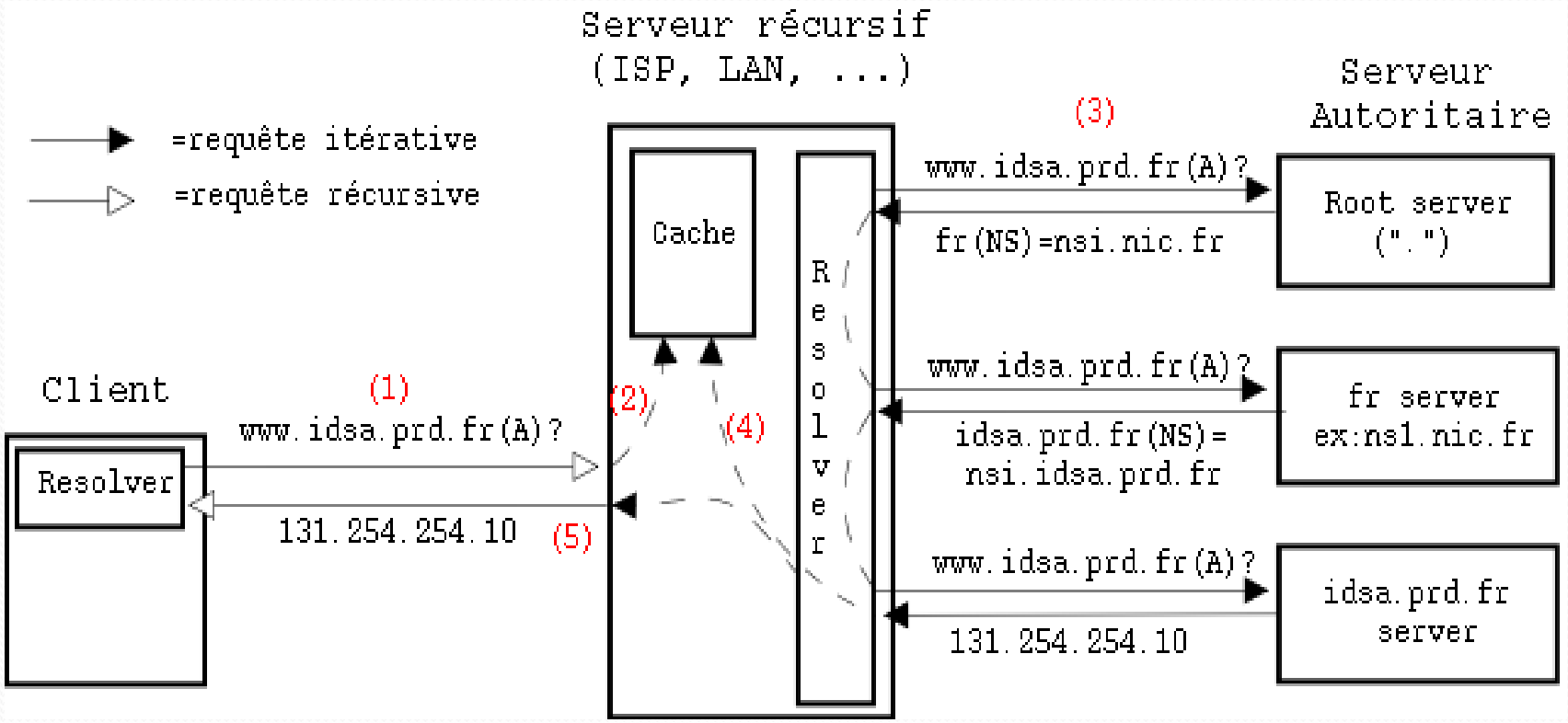


Packet DNS



DNS packet on the wire

Resolution DNS



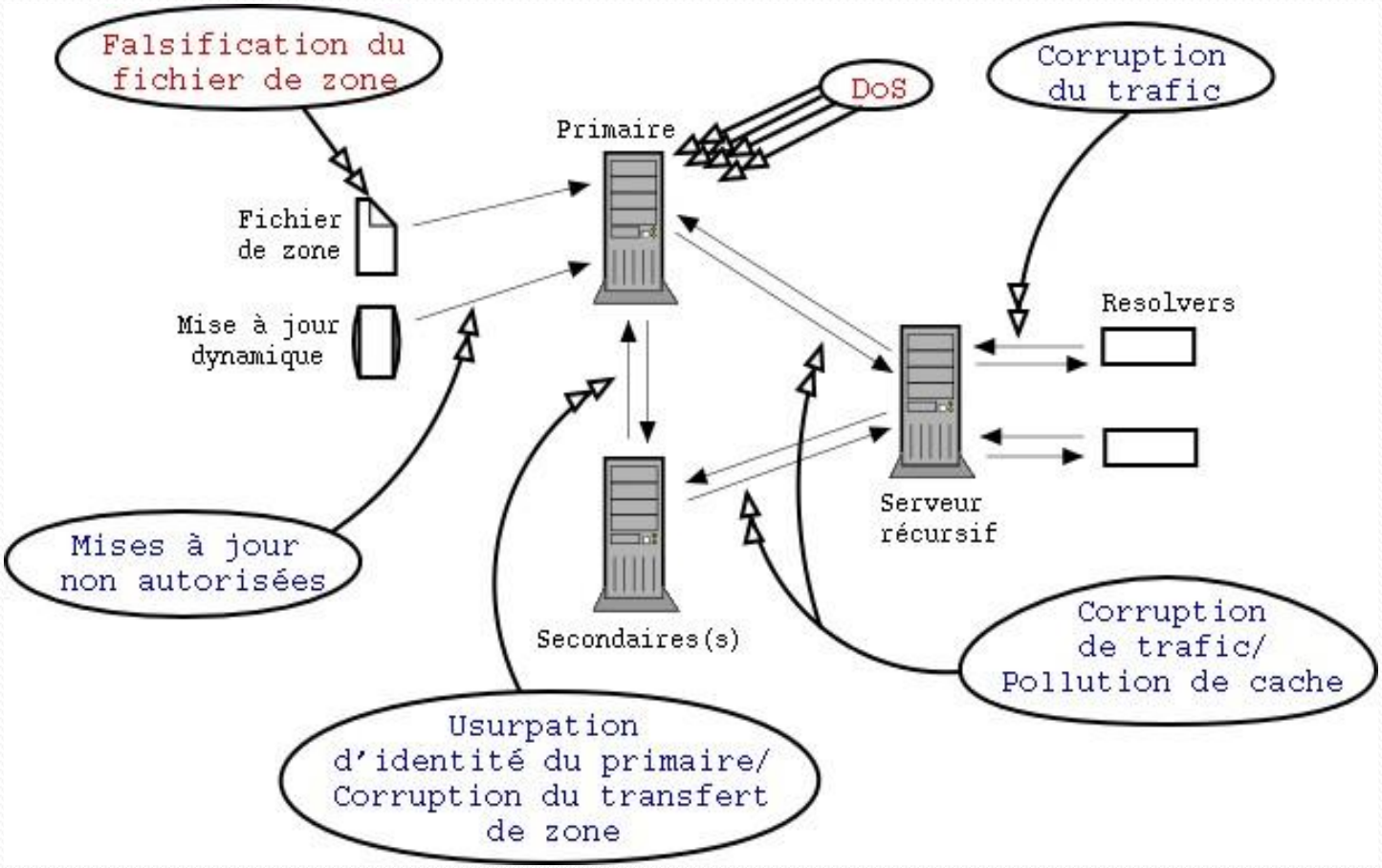
Dns : Préparation/Délégation

Lab 0/1

Les failles de sécurité

- Nature publique des données/ accès universel
- Disponibilité des données
- Authenticité et intégrité
- Attaques spécifiques/non spécifiques au DNS

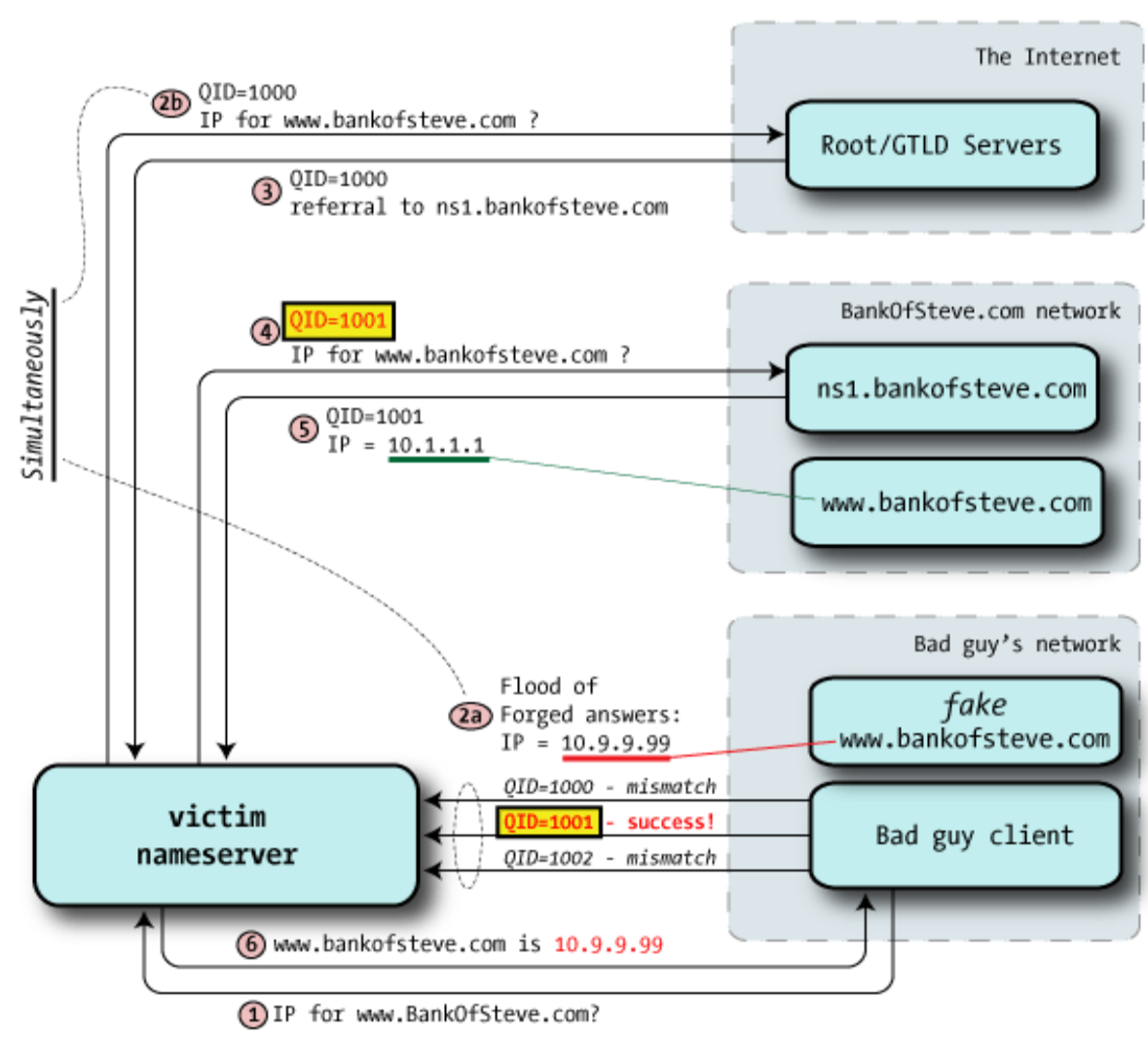
Vulnérabilités de l'architecture DNS



Impacte

- Perturber ou bloquer le service DNS
- Empêcher l'accès à certains équipements
- Rediriger les utilisateurs à leur insu : préambule à une attaque plus grave
- Récupérer des informations critiques

Exemple de Kaminsky



Sécurité DNS : ACL

- ACL est un goupe d'addresse/reseaux IPv4/IPv6 servant a :
  - Simplifier la configuration de bind.
  - Eviter les duplications.
  - Restreindre l'utilisation des options de bind.
  - Offrir plus de sécurité.

  Exemple :

  acl "moreips" { 10.0.0.1; 192.168.23.128/25; };

Sécurité DNS : TSIG

- Transaction SIGnature (RFC 2845) : meta RR
- Secret partagé (cryptographie symétrique)
- Signature d'un hash (algorithme HMAC-MD5)
- Authenticité et intégrité
- Nécessite une synchronisation du temps : NTP
- Utilisation limiter entre le master et le slave : ne peux pas protéger les résolveurs.
- Facile a déployer.

TSIG : Utilisation

- Générer une clef (dnssec-keygen)

  #dnssec-keygen -a <algorithm> -b <bits> -n host <key name>
- Transmettre cette clef secrète au serveur secondaire (email, scp, etc..)
- Configurer les serveurs master et slave avec la même clef.

TSIG : exemple

Master →

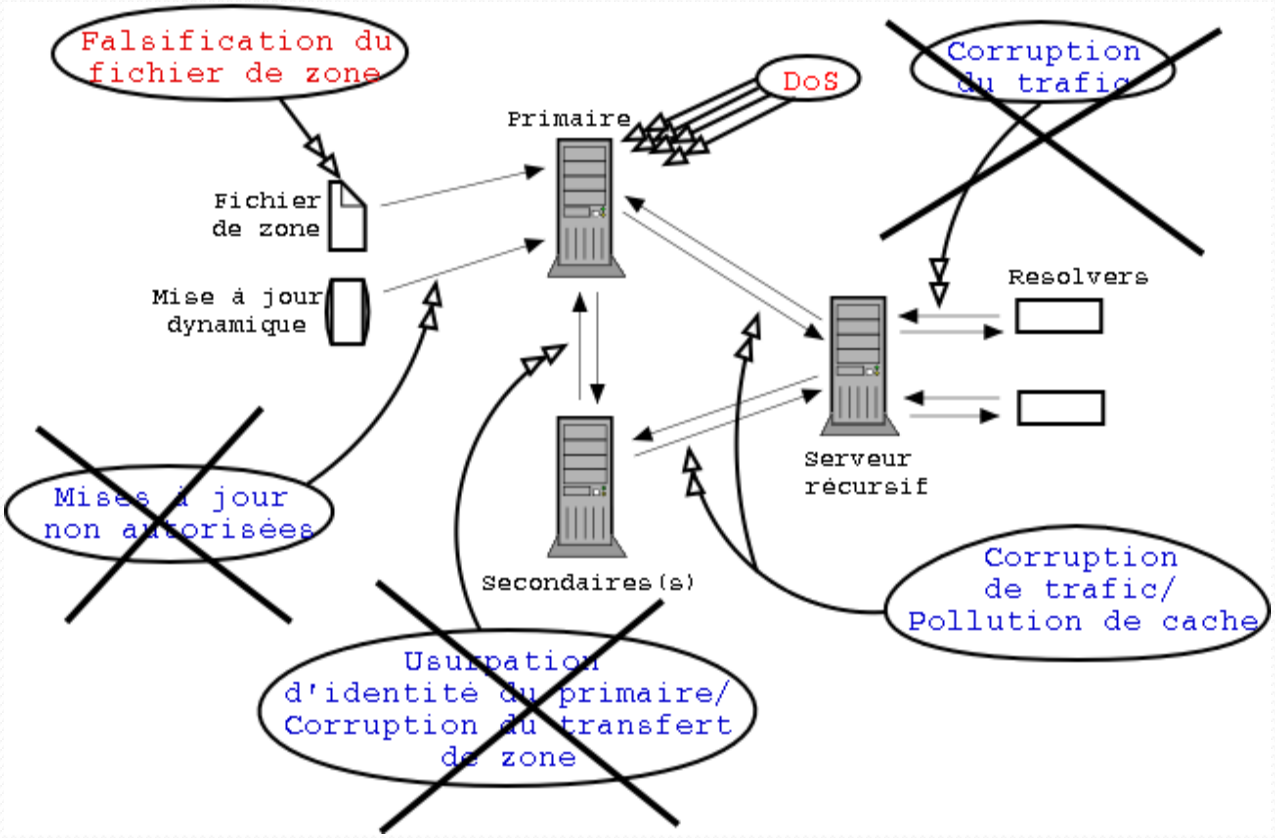
```
key "transfer-key" {
        algorithm hmac-md5;
        secret "sAfRkDLdld56lfD5LvD46DxlFm6flS=";
};
zone confiance.fr {
        type master;
        file "db.confiance.fr";
        allow-transfer { key transfer-key; };
}
```

Slave →

```
key "transfer-key" {
        algorithm hmac-md5;
        secret "sAfRkDLdld56lfD5LvD46DxlFm6flS=";
server 192.249.249.1 {
        keys { transfer-key; };
};
zone confiance.fr {
        type slave;
        file "db.confiance.fr";
        masters { 192.249.249.1; };
};
```

Attention : Secret, algorithme et nom affectés à la clé doivent être identiques sur Master et Slave

TSIG : Vulnérabilités résolues



Renforcer la sécurité :

- Utilisation des ACL
  - Limiter/Filtrer les sources de problèmes (IP)

- Utilisation du TSIG :
  - Protéger les transactions (requêtes dns)

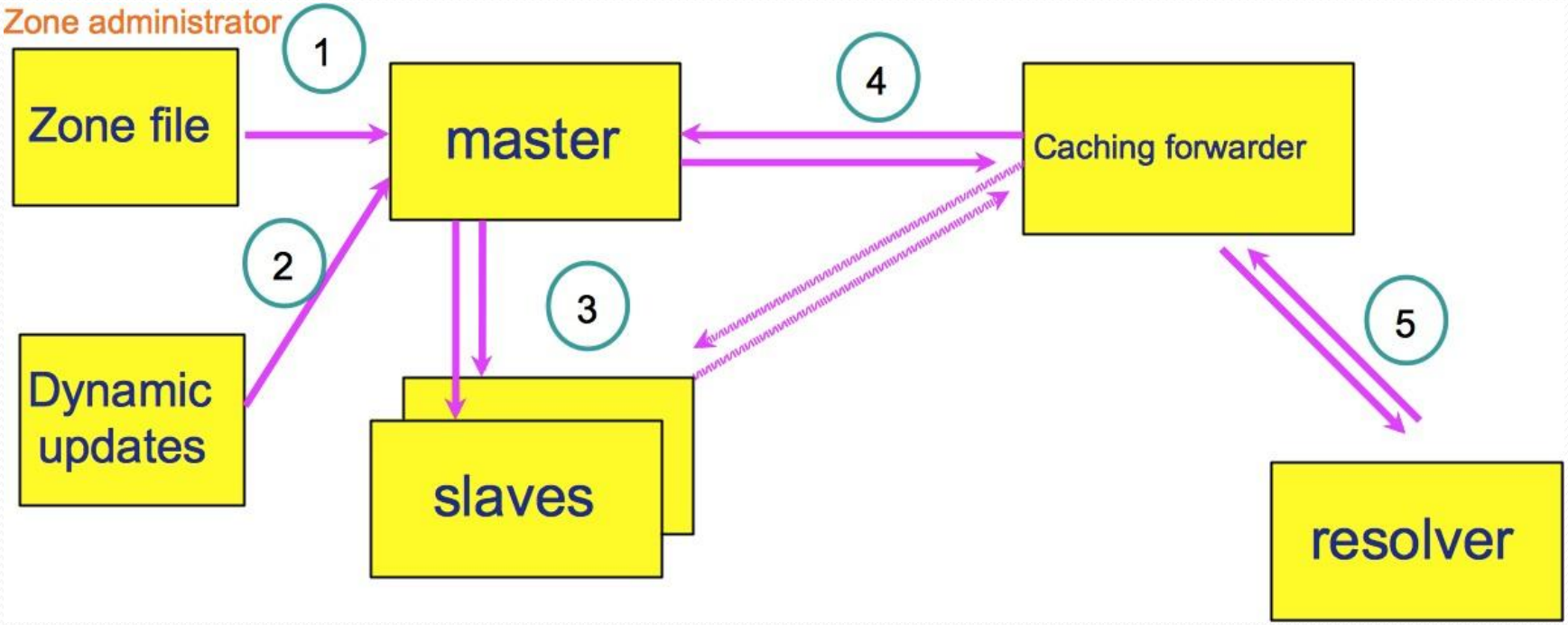
- Masquer la version de bind :
  - Masquer les vulnérabilités

Suffisant ??

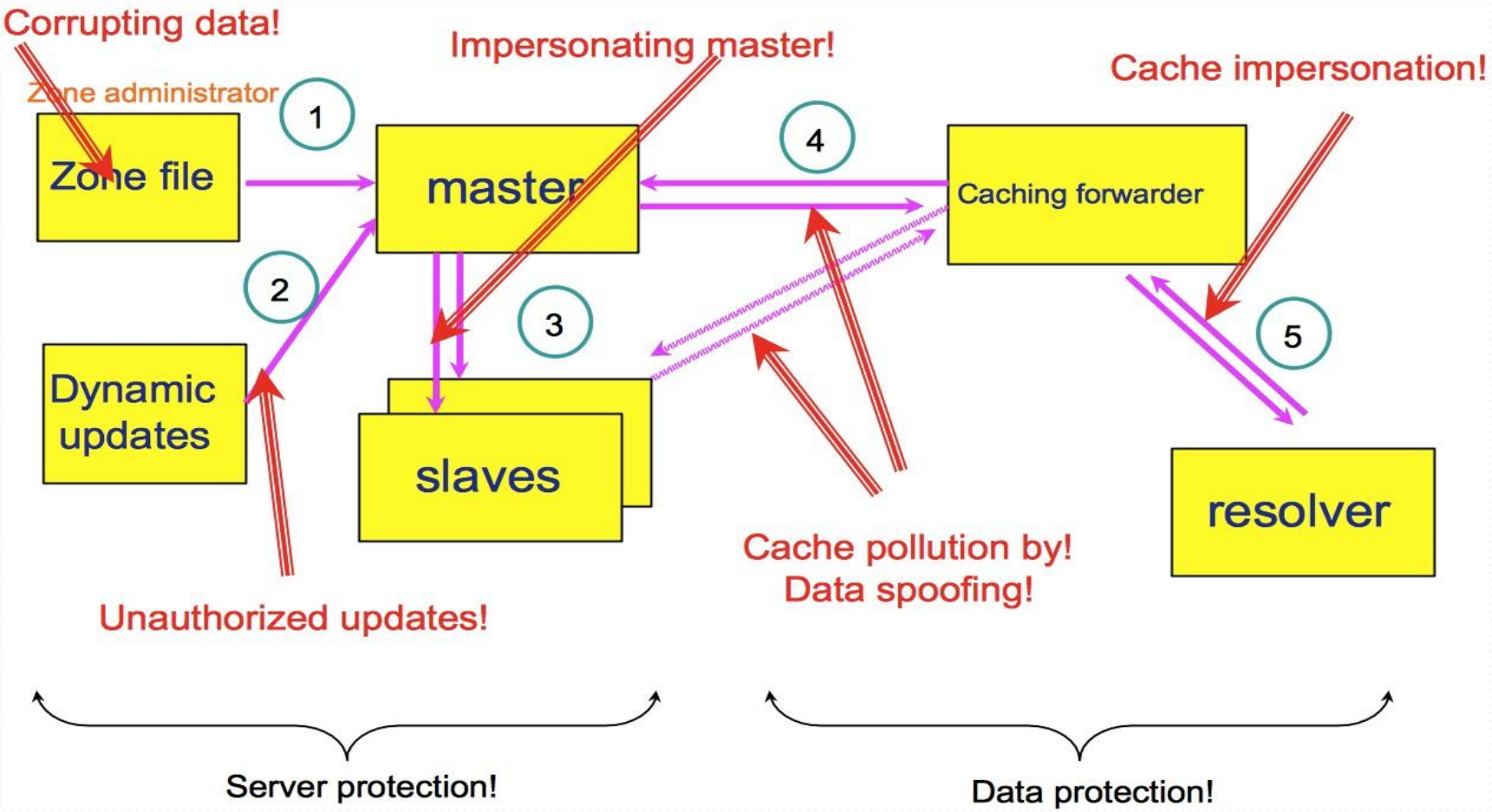
Sécurité DNS

Lab 2

DNS : Trafic


Zone administrator
1
Zone file
master
4
Caching forwarder
2
3
5
Dynamic updates
slaves
resolver

DNS : Vulnerabilities

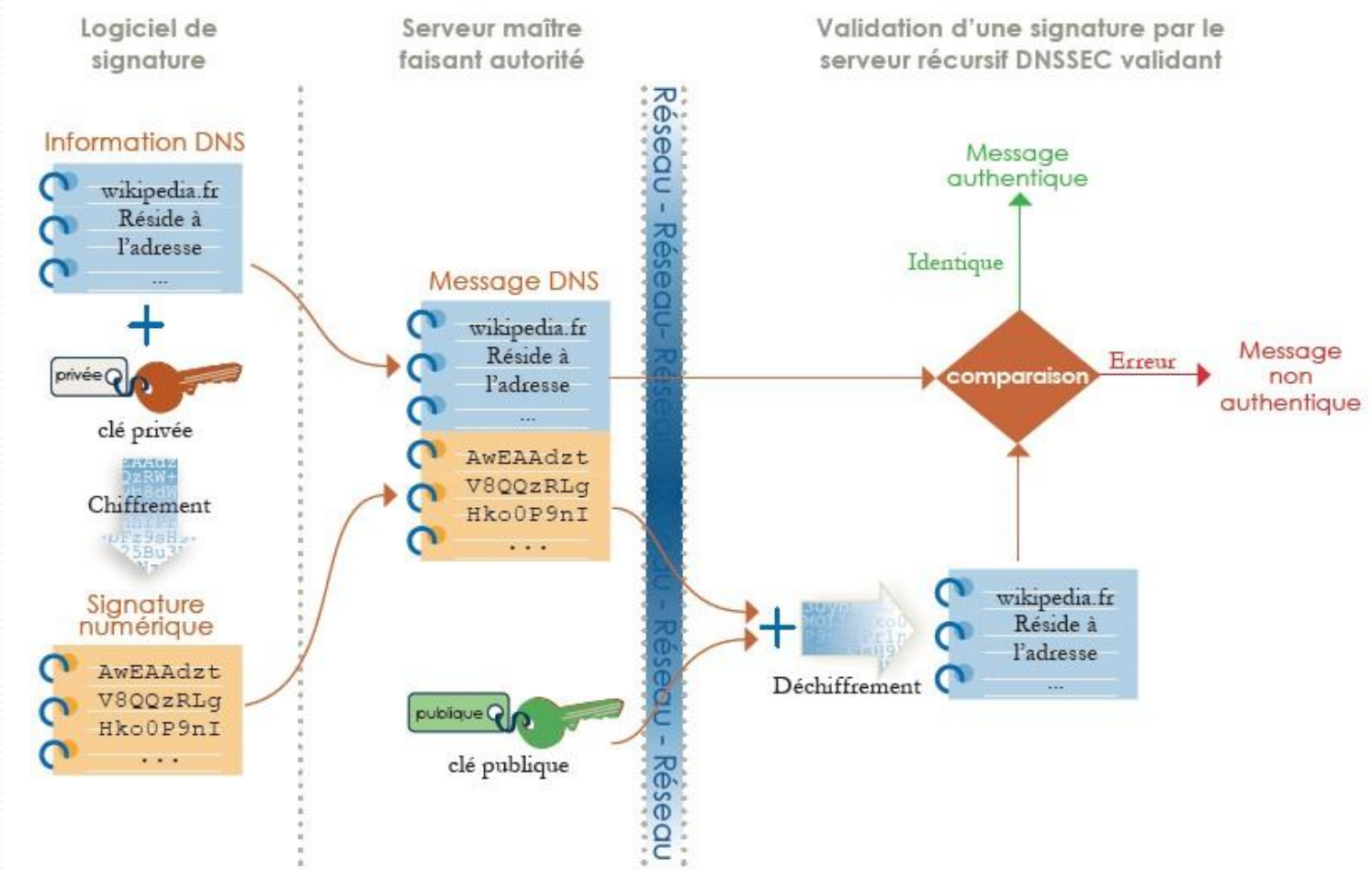


DNSSEC

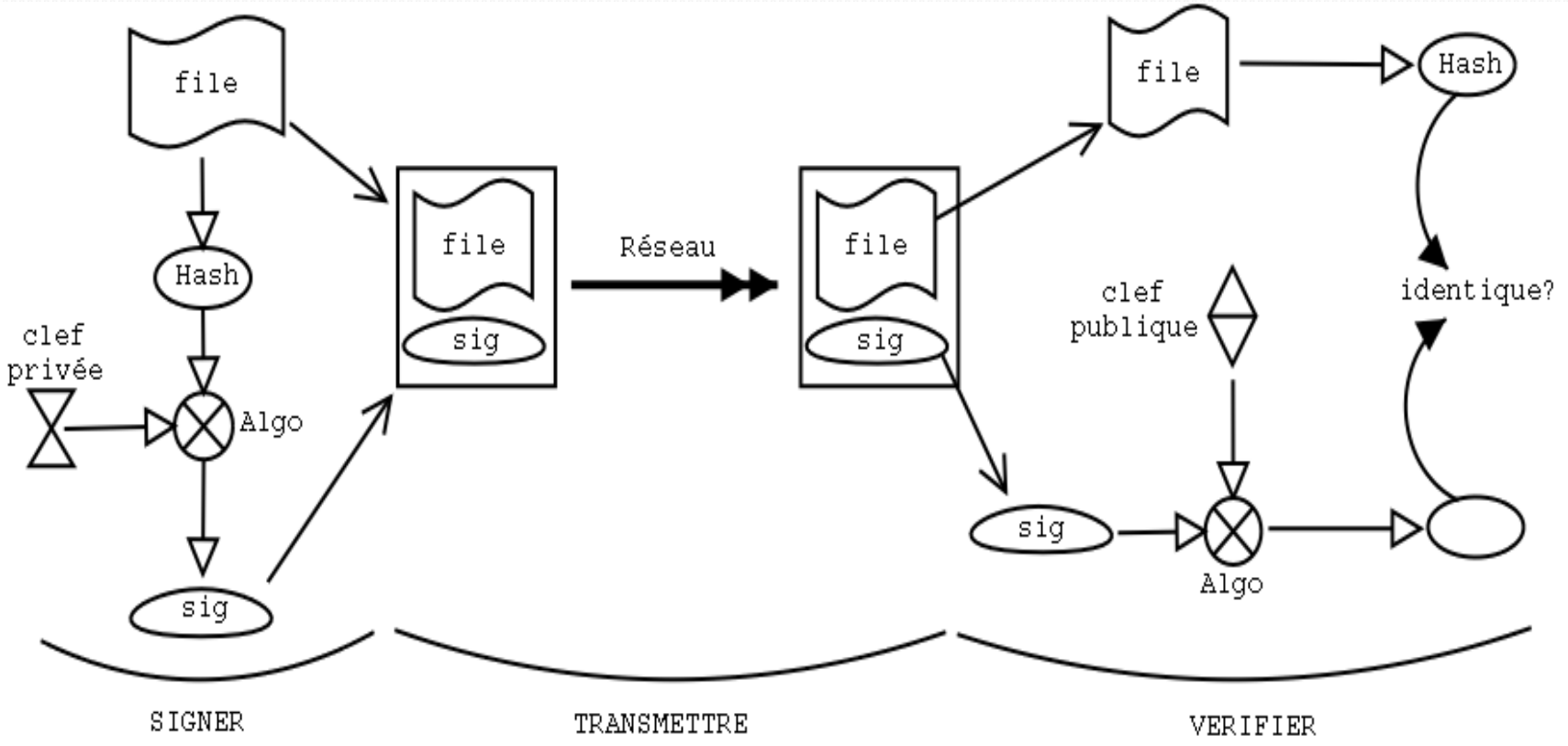
DNSSEC : Rôle

- Authenticité et intégrité des données en signant les ensembles d'enregistrements de ressources avec une clé privée.
- Sécurité des transactions en utilisés des cles publics pour vérifier les RRSIG.
- Architecture de distribution des clefs.
- Outils basés sur la cryptographie.

DNSSEC : Fonctionnement



DNSSEC : Cryptographie



DNSSEC : Sécurité Serveur

- Chaque zone génère un ensemble de paires de clefs (partie privée/partie publique)

- Les parties privées des clefs signent les informations (RRsets) faisant partie intégrante de la zone

- Les signatures sont stockées dans le fichier de zone en compagnie des données qu'elles authentifient

- Les parties publiques des clefs sont publiées dans le fichier de zone et peuvent faire l'objet de requêtes DNS standard

DNSSEC : Sécurité Client

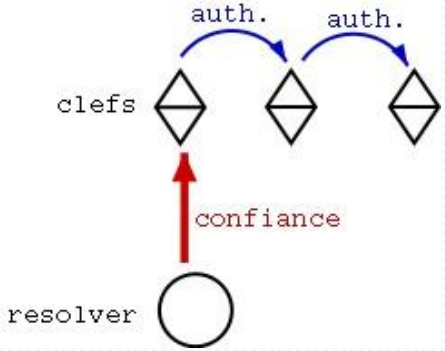
- La connaissance de la clef publique d'une zone permet de vérifier les signatures et donc l'authenticité et l'intégrité des informations contenues dans la zone

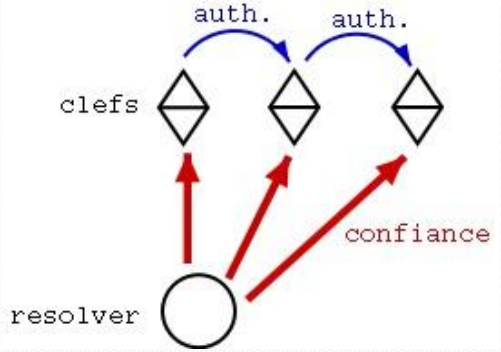
- Concept de clef de confiance (Client-Serveur)

- Limitations : nécessite la connaissance des clefs de toutes les zones avec lesquelles le résolveur est susceptible de communiquer

DNSSEC : Sécurité Global

- Authentification des clefs en cascade
- Structure arborescente du DNS idéale
- Délégations sécurisées et chaînes de confiance





DNSSEC : Les Clés

- Utilisation des clés pour garder l'authenticité et l'intégrité des réponses.
- DNSSEC utilise le système de cryptographie à clé publique.
- DNSSEC utilise deux types de clés.
  - Clé pour signer les données (enregistrements)
  - Clé pour signer les clés (dnskey)

- Les Clés sont distingués par l'algorithme et la longueur utilisés.
- Les Clés n'expirent jamais mais la signature expire.

DNSSEC : ZSK

- La Zone Signing Key (ZSK) correspond à la clé privée utilisée pour signer une zone.
  - ZSK Signe les enregistrements et RRset.
- La clé publique correspondante est connue des serveurs récursifs afin qu'ils puissent vérifier les hash des réponses.
- La ZSK a une validité déterminée : elle doit être renouvelé régulièrement.

DNSSEC : KSK

- La Key Signing Key est une clé privée destinée à signer la (ZSK). Une KSK n'est utilisée que pour signer un enregistrement DNSKEY.

- La clé KSK fait office de maillon de confiance dans la chaîne de confiance.

- La KSK a une validité déterminée : elle doit être renouvelé régulièrement. (plus long que la ZSK)

DNSSEC : STOCKAGE

- La gestion des clés privées est un des principaux problèmes rencontrés lors du déploiement de DNSSEC.
- Les problèmes rencontrés sont identiques à ceux rencontrés lors du déploiement de n'importe quelle P.K.I (public key infrastructure).
- La sécurité de DNSSEC reposant sur le secret contenu dans les clés privées KSK et ZSK, celles-ci doivent être stockées à des endroits non connectés au réseau.
- Les clés publiques sont stockées dans les enregistrements DNSKEY.

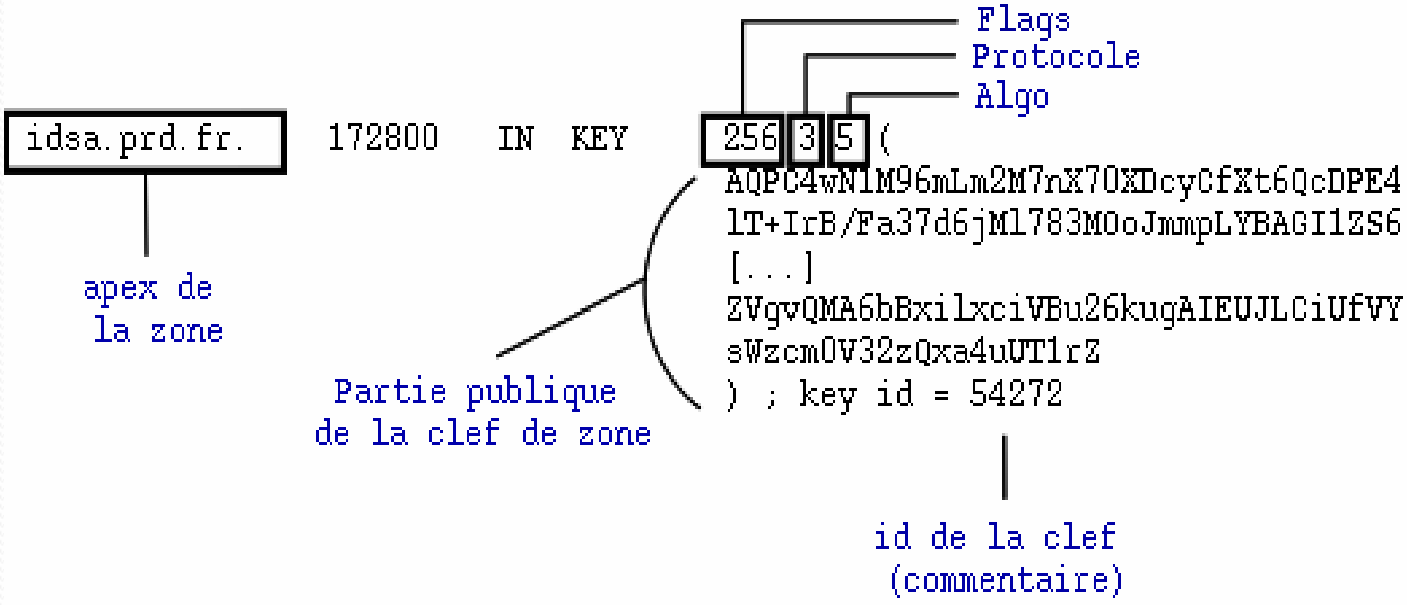
DNSSEC : Manual Signing

Lab 4

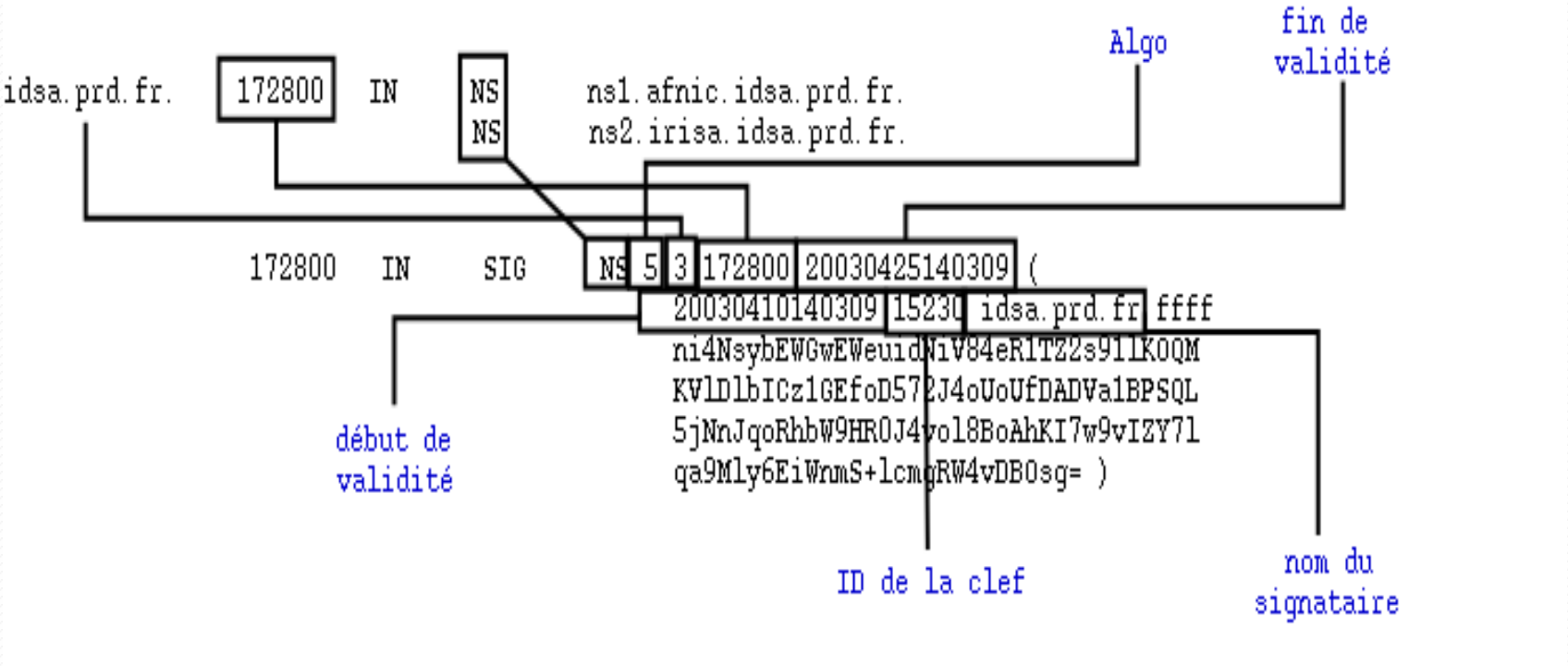
DNSSEC : Nouveautés

- DNSSEC a apporté de nouveaux RR tel que :
  - DNSKEY, RRSIG : sécuriser les RRsets
  - NSEC/NSEC3 : garantir la complétude d'une zone
  - DS : établir des chaînes de confiance
- DNSSEC a apporté la notion de signature et clés :
  - ZSK : zone signing key
  - KSK : key signing key
- DNSSEC a apporté de nouveaux flags tel que :
  - (CD, AD, DO)

DNSSEC : Format DNSKEY



DNSSEC : Format RRSIG



DNSSEC : Signature

```
test.com.       SOA         ns.test.com.      root.test.com. (
                               2009041800 1h 10m 30d 1d )
                NS          ns.test.com.
                A           10.0.0.1
                MX          0 mail.test.com.
ns              A           10.0.0.1
mail            A           10.0.0.2
www             A           10.0.0.3
ftp             CNAME       www.test.com.
west            NS          ns.west.test.com.
ns.west         A           10.0.0.5
east            NS          ns.east.test.com.
ns.east         A           10.0.0.6
```

DNSSEC : Signature

```
test.com.                SOA     ns.test.com.     root.test.com. (
                                    2009041800 1h 10m 30d 1d )
test.com.                NS      ns.test.com.
test.com.                A       10.0.0.1
test.com.                MX      0 mail.test.com.
east.test.com.           NS      ns.east.test.com.
ns.east.test.com.        A       10.0.0.6
ftp.test.com.            CNAME   www.test.com.
mail.test.com.           A       10.0.0.2
ns.test.com.             A       10.0.0.1
west.test.com.           NS      ns.west.test.com.
ns.west.test.com.        A       10.0.0.5
www.test.com.            A       10.0.0.3
```

DNSSEC : Signature

```
test.com.               SOA     ns.test.com. root.test.com. (
                           2009041800 1h 10m 30d 1d )
test.com.               NS      ns.test.com.
test.com.               A       10.0.0.1
test.com.               MX      0 mail.test.com.
test.com.               NSEC    east.test.com. A NS SOA MX NSEC
east.test.com.          NS      ns.east.test.com.
east.test.com.          NSEC    ns.east.test.com. NS NSEC
ns.east.test.com.       A       10.0.0.6
ns.east.test.com.       NSEC    ftp.test.com. A NSEC
ftp.test.com.           CNAME   www.test.com.
ftp.test.com.           NSEC    mail.test.com. CNAME NSEC
mail.test.com.          A       10.0.0.2
mail.test.com.          NSEC    ns.test.com. A NSEC
ns.test.com.            A       10.0.0.1
ns.test.com.            NSEC    west.test.com. A NSEC
west.test.com.          NS      ns.west.test.com.
west.test.com.          NSEC    ns.west.test.com. NS NSEC
ns.west.test.com.       A       10.0.0.5
ns.west.test.com.       NSEC    www.test.com. A NSEC
www.test.com.           A       10.0.0.3
www.test.com.           NSEC    test.com. A NSEC
```

DNSSEC : Signature

- Si on demande un Non-Existant domain :

mail.test.com. *NSEC* *ns.test.com.* *A* *NSEC*

- Si on demande un Non-Existant type :

mail.test.com. *NSEC* *ns.test.com.* *A* *NSEC*

NB : NXDOMAIN : signifie que l'enregisrement ou/et le type n'existe pas pour le domain en question.

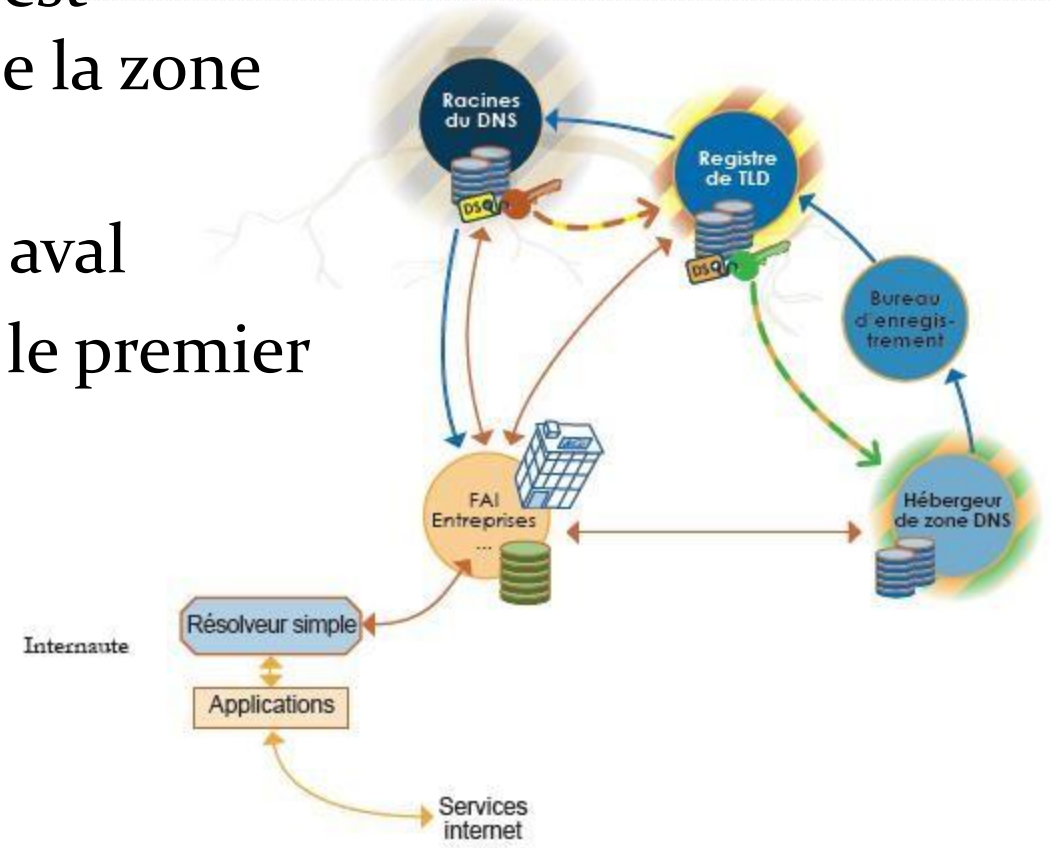
DNSSEC : Signature

```
example.com.            SOA     <SOA stuff>
example.com.            NS      ns1.secure-hoster.net.
example.com.            NS      ns2.secure-hoster.net.
example.com.            A       192.45.56.67
example.com.            MX      10 mail.example.com.
mail.example.com.       A       192.45.56.68
www.example.com.        A       192.45.56.67
```

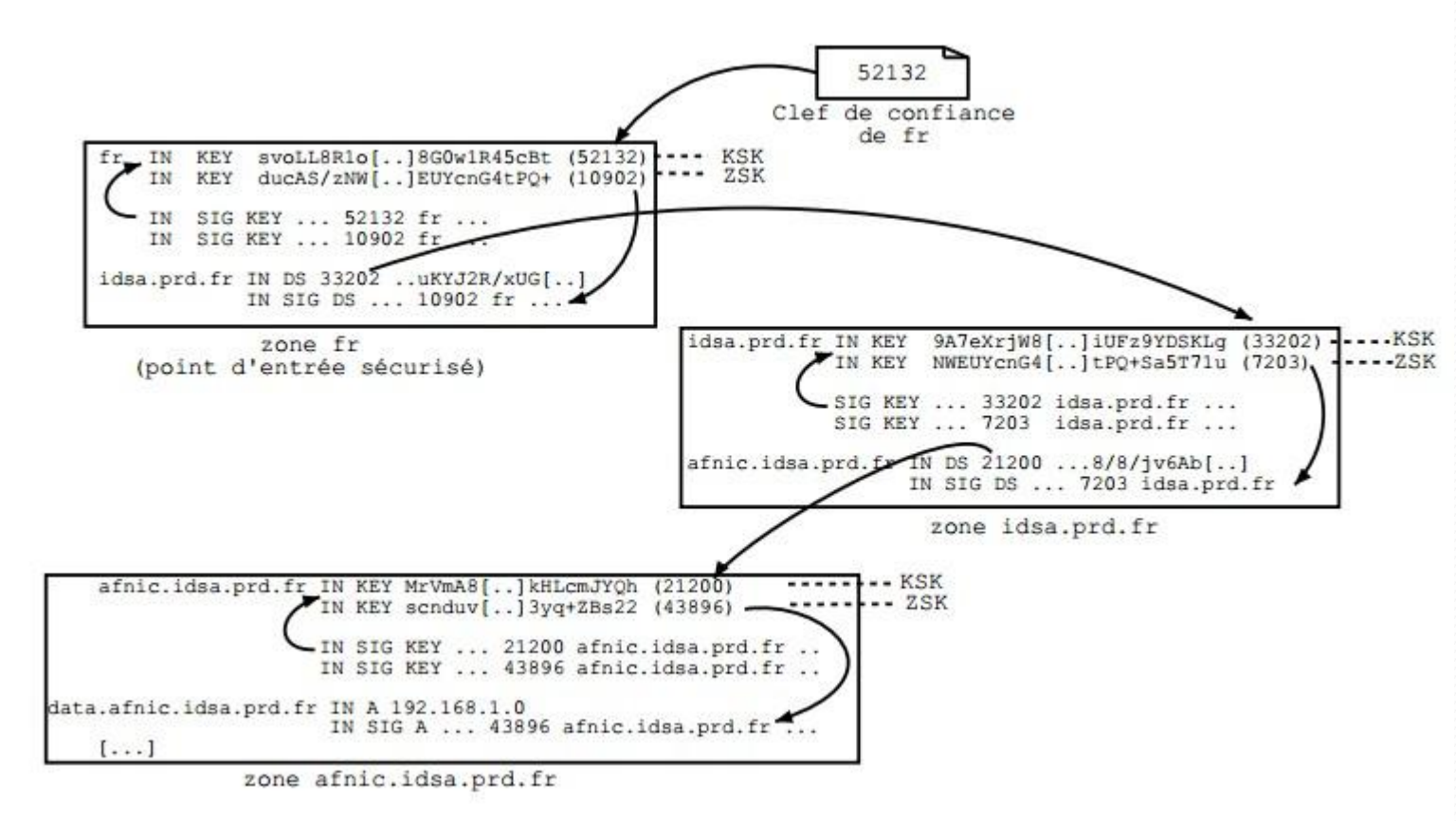
```
example.com.            SOA     <SOA stuff>
example.com.            RRSIG   SOA <RRSIG stuff>
example.com.            NS      ns1.secure-hoster.net.
example.com.            NS      ns2.secure-hoster.net.
example.com.            RRSIG   NS <RRSIG stuff>
example.com.            A       192.45.56.67
example.com.            RRSIG   A <RRSIG stuff>
example.com.            MX      10 mail.example.com.
example.com.            RRSIG   MX <RRSIG stuff>
example.com.            DNSKEY  <Key that signs example.com DNSKEY RRSet>     ; KSK
example.com.            DNSKEY  <Key that signs the rest of example.com zone> ; ZSK
example.com.            RRSIG   DNSKEY <RRSIG stuff>
example.com.            NSEC    mail.example.com. SOA NS A MX DNSKEY RRSIG NSEC
example.com.            RRSIG   NSEC <RRSIG stuff>
mail.example.com.       A       192.45.56.68
mail.example.com.       RRSIG   A <RRSIG stuff>
mail.example.com.       NSEC    www.example.com. A RRSIG NSEC
mail.example.com.       RRSIG   NSEC <RRSIG stuff>
www.example.com.        A       192.45.56.67
www.example.com.        RRSIG   A <RRSIG stuff>
www.example.com.        NSEC    example.com. A RRSIG NSEC
www.example.com.        RRSIG   NSEC <RRSIG stuff>
```

DNSSEC : 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
- La chaine est cassé dès le premier échec de validation.



DNSSEC : Chaine de Confiance



DNSSEC : Nécessités

- Nécessité d'un niveau de sécurité intrinsèque des serveurs. Le déploiement de DNSSEC devrait donc indirectement augmenter le niveau de sécurité des serveurs
- Nouveaux enjeux : maintenance -Automatisation des procédures -Surveillance -Responsabilité dans les chaînes de confiance -Précautions pour la gestion des clefs
- Procédure la plus délicate : le roulement des clés

DNSSEC : Roulement des clés

- Possibilité de compromission des clés -perte ou vol de la partie privée -attaques cryptanalytiques.
- Roulement planifié/ roulement d'urgence.
- Efficacité du modèle ZSK/KSK.
- Précautions concernant les temps caractéristiques (validité des SIGs, intervalle de resignature, TTLs)

DNSSEC : Roulement ZSK

- ZSK de petite taille ÎRoulementfréquent et régulier
- Ce roulement est local à la zone (pas d'interactions avec la zone parente)
- Contraintes à considérer : les TTLs et la propagation des données dans les caches
- Procédure conseillée : pré-publication de la future clef + post-suppression de l'ancienne clé

DNSSEC : Roulement KSK

- Prépublication de la nouvelle KSK (idem procédure ZSK)
- Transmission de la nouvelle KSK à la zone parente
- Ne pas rompre la chaîne de confiance : le changement de DS doit être propagé dans les caches. Pendant cette durée, il est souhaitable que la zone fille utilise simultanément les deux KSK ou que la zone parente publie 2 DS
- Communiquer sur le changement de clé car certains résolveurs avaient configuré l'ancienne clé comme clé de confiance
- Ce rollover nécessite une bonne synchronisation des zones fille et parente

DNSSEC : Outils

- Utilisation de BIND9.3s (snapshots) et ses outils
  - -dnssec-keygen
  - -dnssec-signzone
- Temps de signature reste raisonnable même pour des zones de grande taille
- Taille de la zone signée: multipliée par un facteur 6 à 10 par rapport au fichier non signé
- Taille des réponses: pour une même requête, une réponse
- DNSsec aura une taille de l'ordre de 5 à 10 fois la taille de la réponse DNS correspondante

DNSSEC : Diagnostique

- http://dnsviz.net/
- http://www.zonemaster.fr
- http://dnssec-debugger.verisignlabs.com/

DNSSEC : Discussion

- Comment vous pouvez planifier votre passage vers DNSSEC ?
- Les Contraintes ?
- Comment ICANN peut vous aider ??