Sécurisation du DNS : les extensions DNSsec

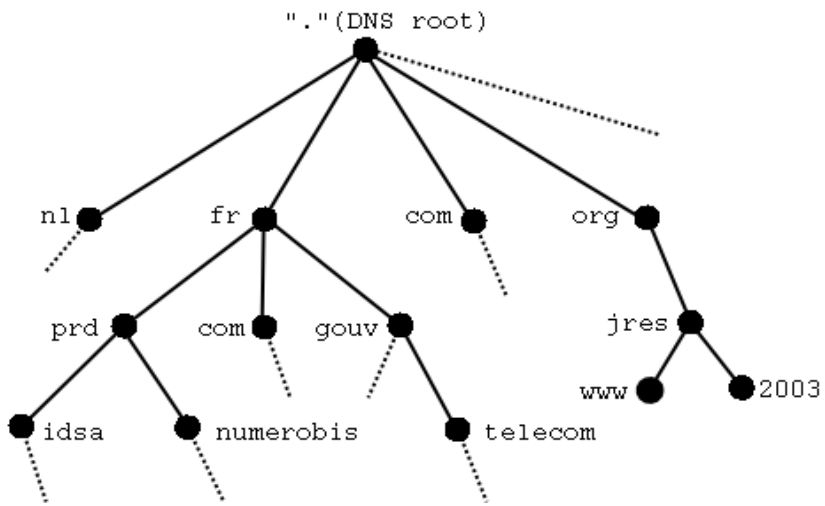
Bertrand Leonard,
AFNIC/projet IDsA

Historique

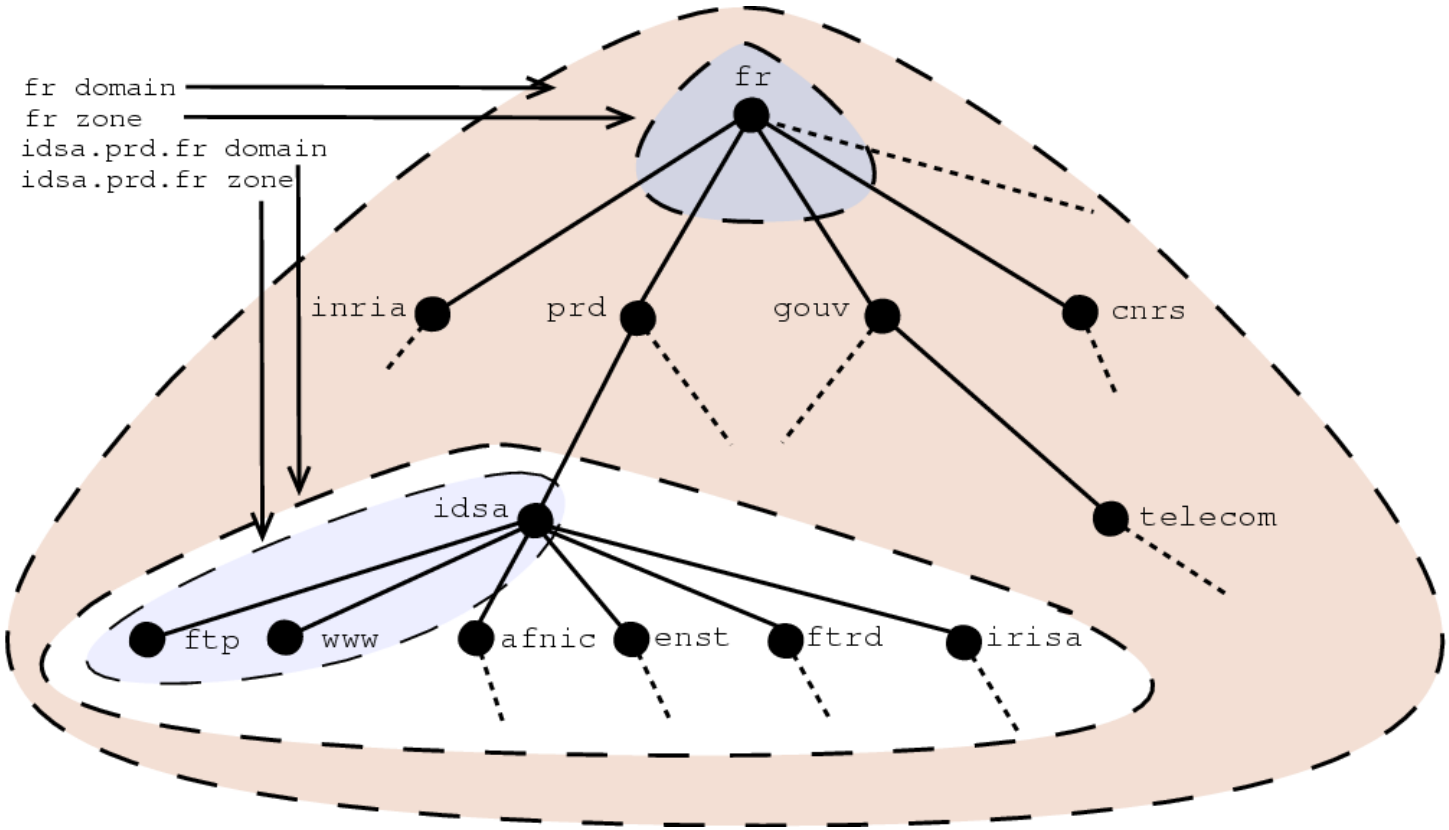
- **Jusqu'en 1984 : réseau restreint militaire/universitaire/recherche**
  - Hôtes de l' ARPAnet/Internet dans un fichier host.txt
  - Mis à jour et diffusé par le SRI-NIC
- **à partir de 1984 : croissance importante du nombre d' hôtes connectés**
  - Limites du modèle précédant
  - Un système de nommage distribué: le DNS
  - RFC 1034/1035 (Paul Mockapetris)
- **1995 : généralisation du réseau et multiplication des usages**
  - Le DNS: un des piliers 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)

Le 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

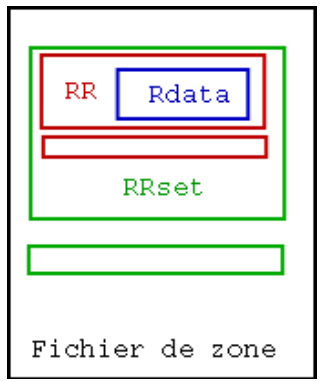


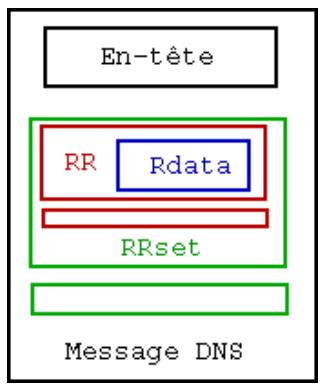
L'arbre DNS (domaines vs zones)



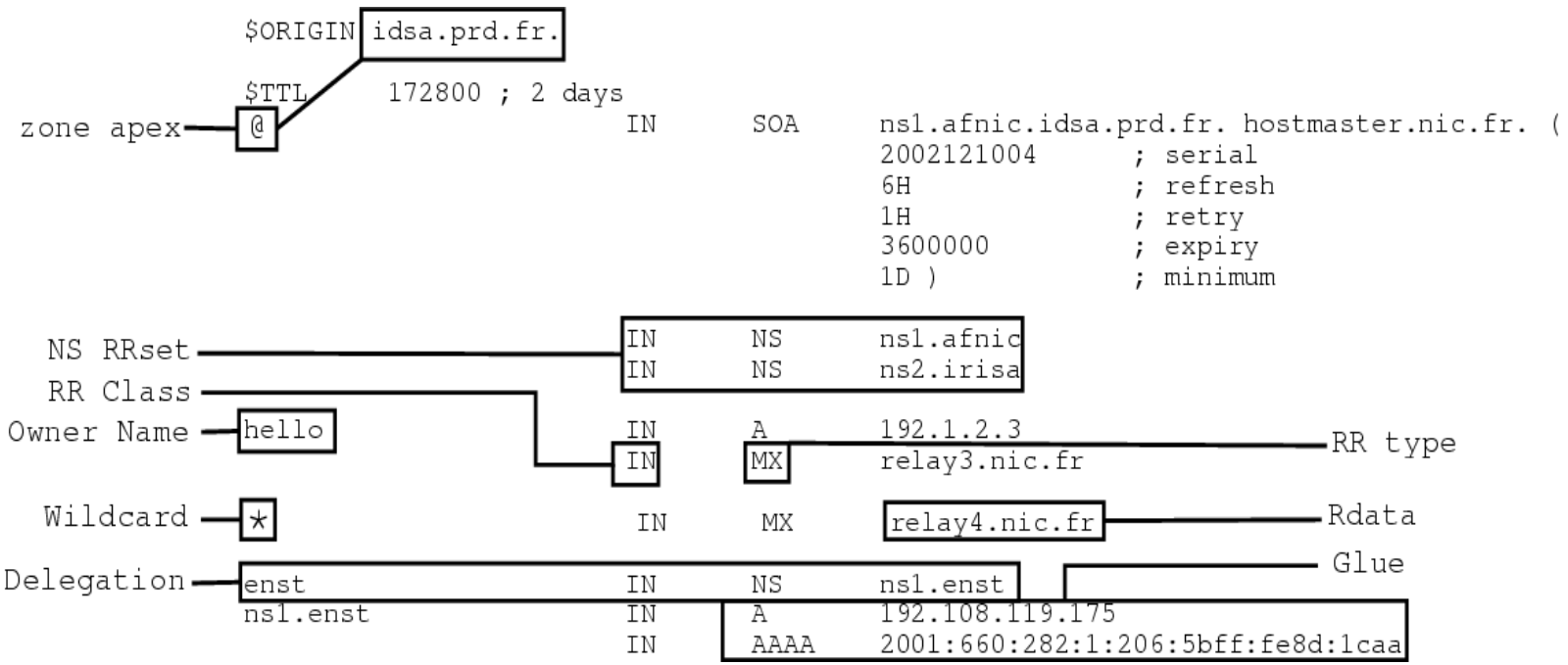
L'information DNS

- Les enregistrements DNS (Resource Records: RRs)
- Les RRsets
- Les fichiers de zone
- Les messages DNS

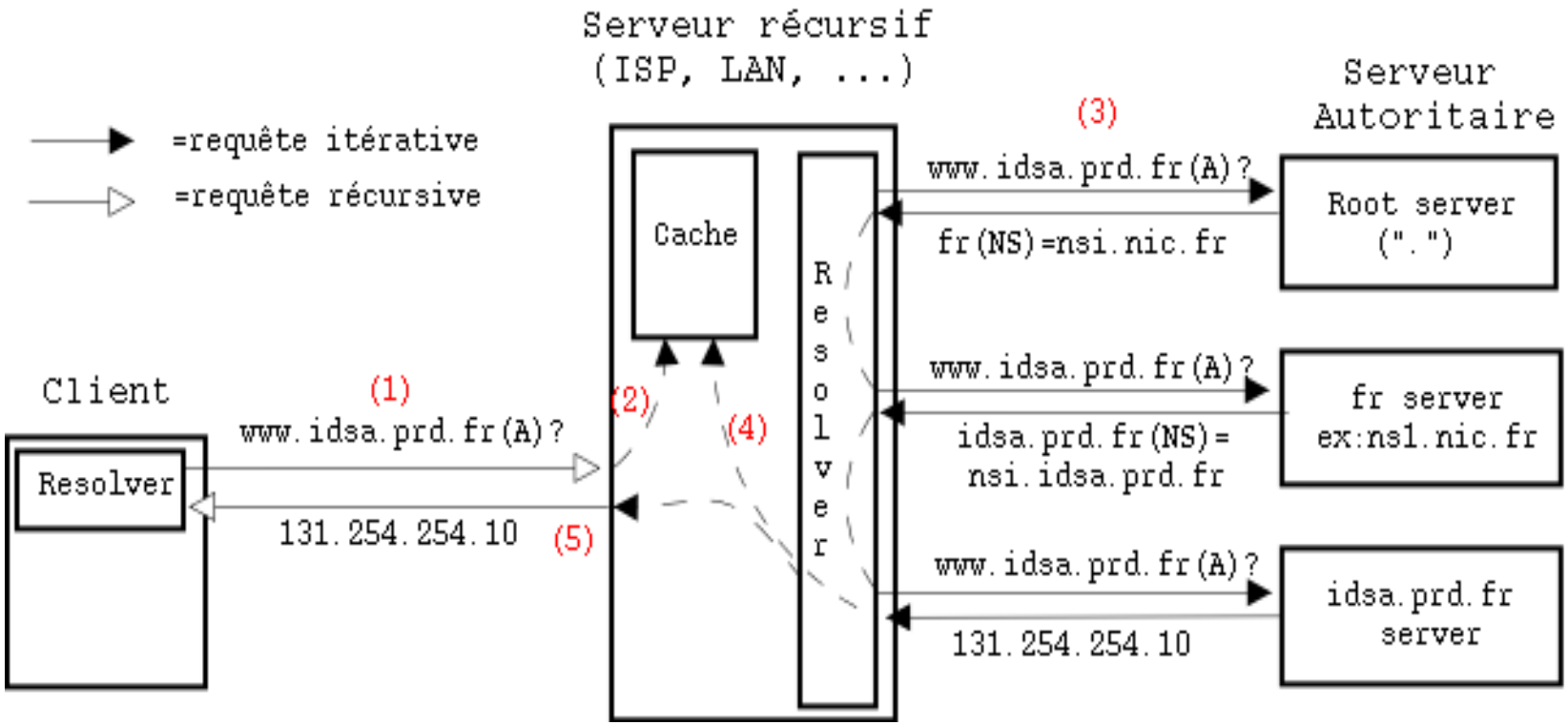




Exemple de fichier de zone



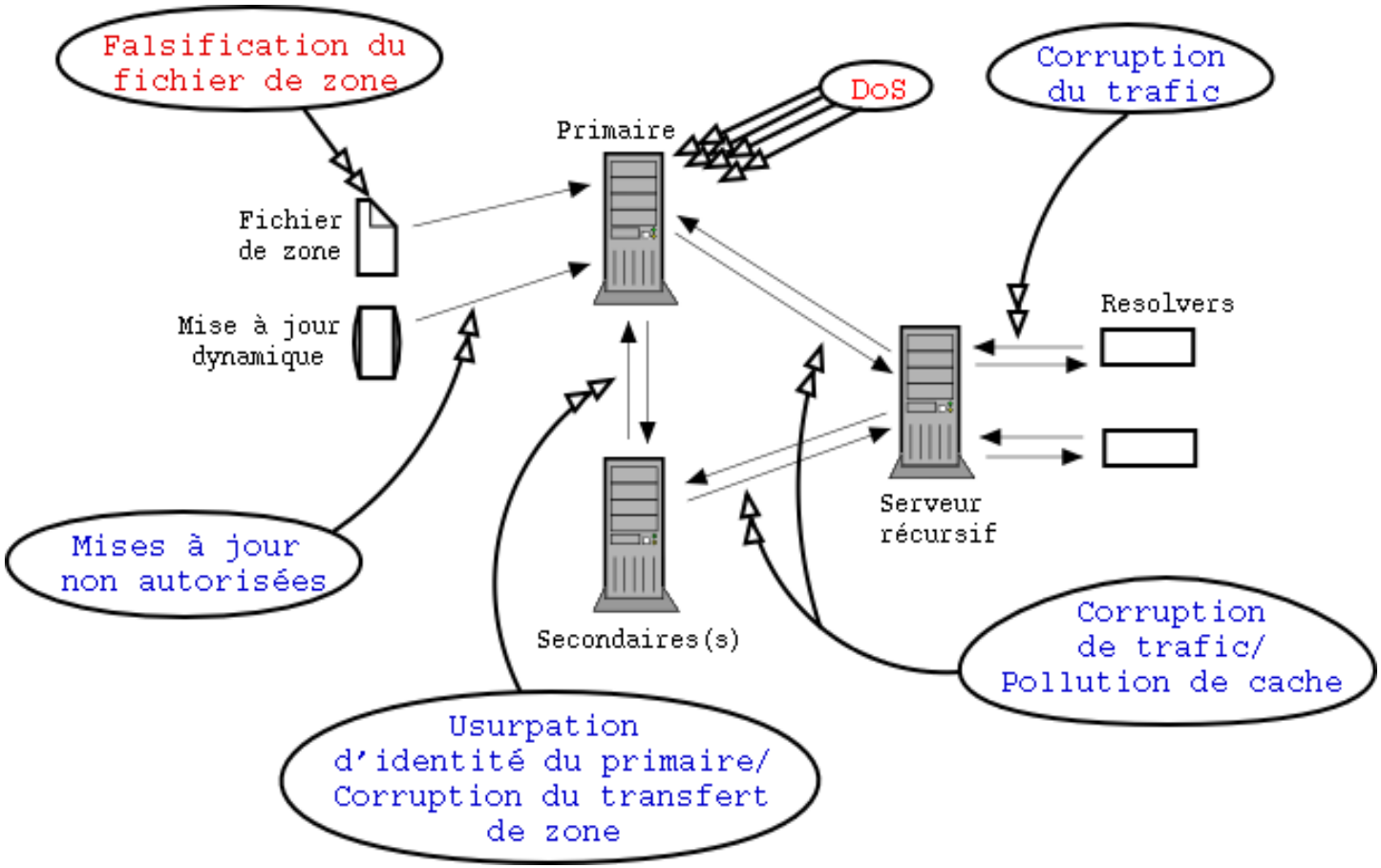
La résolution DNS



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

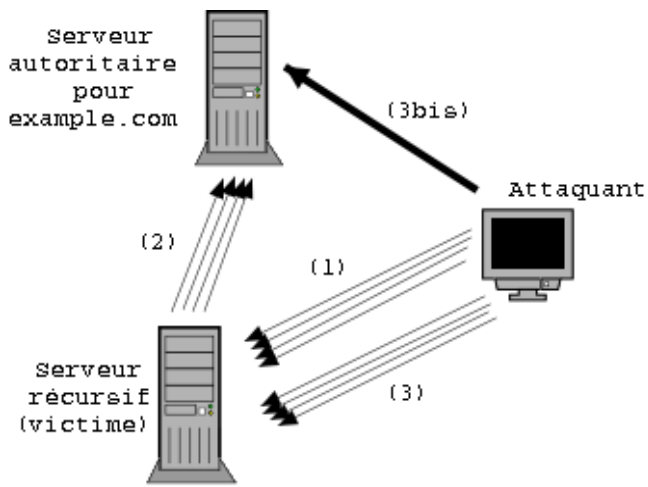


But des attaques

- 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 d'attaque

- Attaques de type “DNS Spoofing”: plusieurs modes opératoires.
  - Man in the middle
  - “Birthday attack”



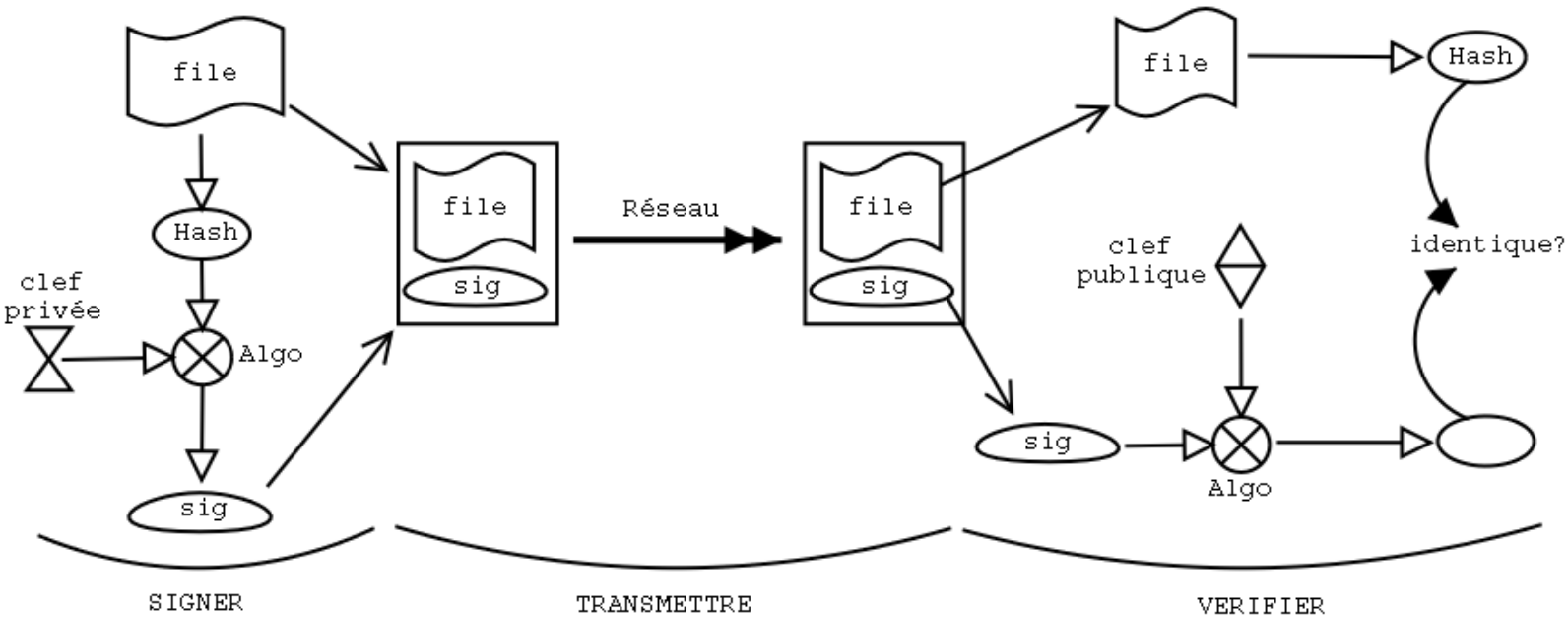
Les services rendus par DNSsec

- Sécurité des données
- Sécurité des transactions (TSIG, SIG(0))
- Architecture de distribution des clefs
- Outils basés sur la cryptographie

Les extensions DNSsec

- Historique
- Authentification de l'origine et intégrité des données
- Distribution de clef (pseudo-PKI)
  - clefs nécessaires au fonctionnement de DNSsec
  - autres clefs (IPsec, SSH, ...)

Rappels de cryptographie à clefs publiques (signatures)



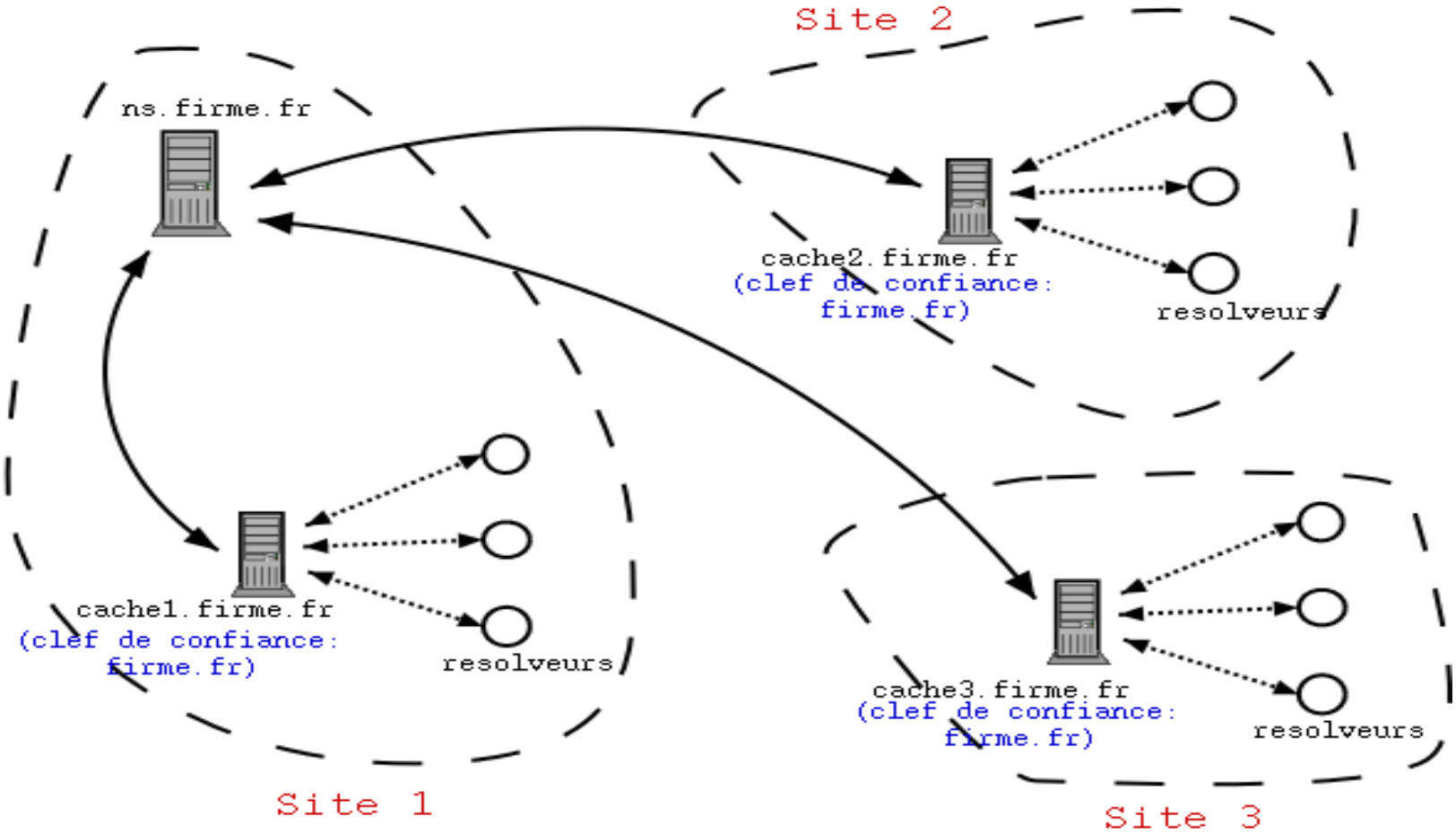
Niveau de sécurité local (côté serveur)

- 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

Niveau de sécurité local (côté 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
- Limitations : nécessite la connaissance des clefs de toutes les zones avec lesquelles le resolver est susceptible de communiquer

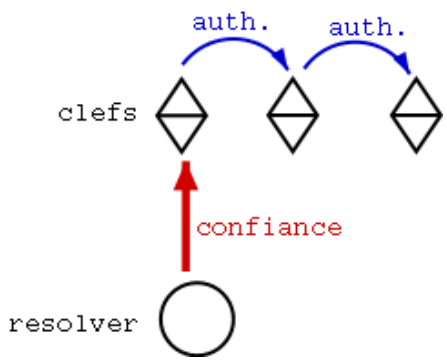
Sécurité locale : exemple



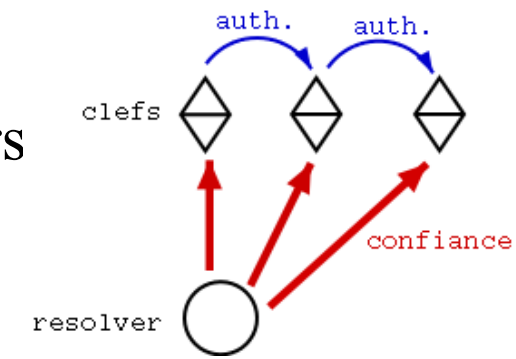
Niveau de sécurité global

- Principe : authentification des clefs en cascade

si



alors

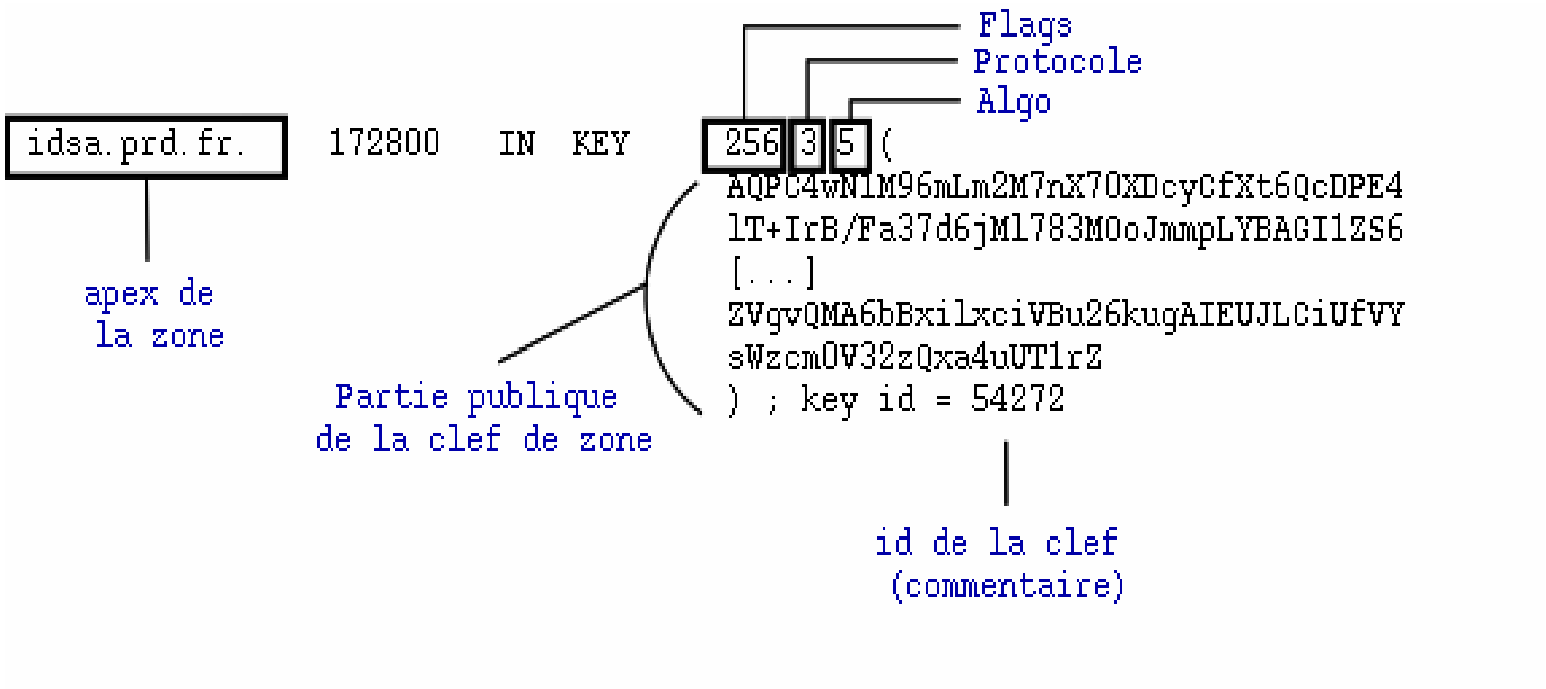


- structure arborescente du DNS idéale
- délégations sécurisées et chaînes de confiance

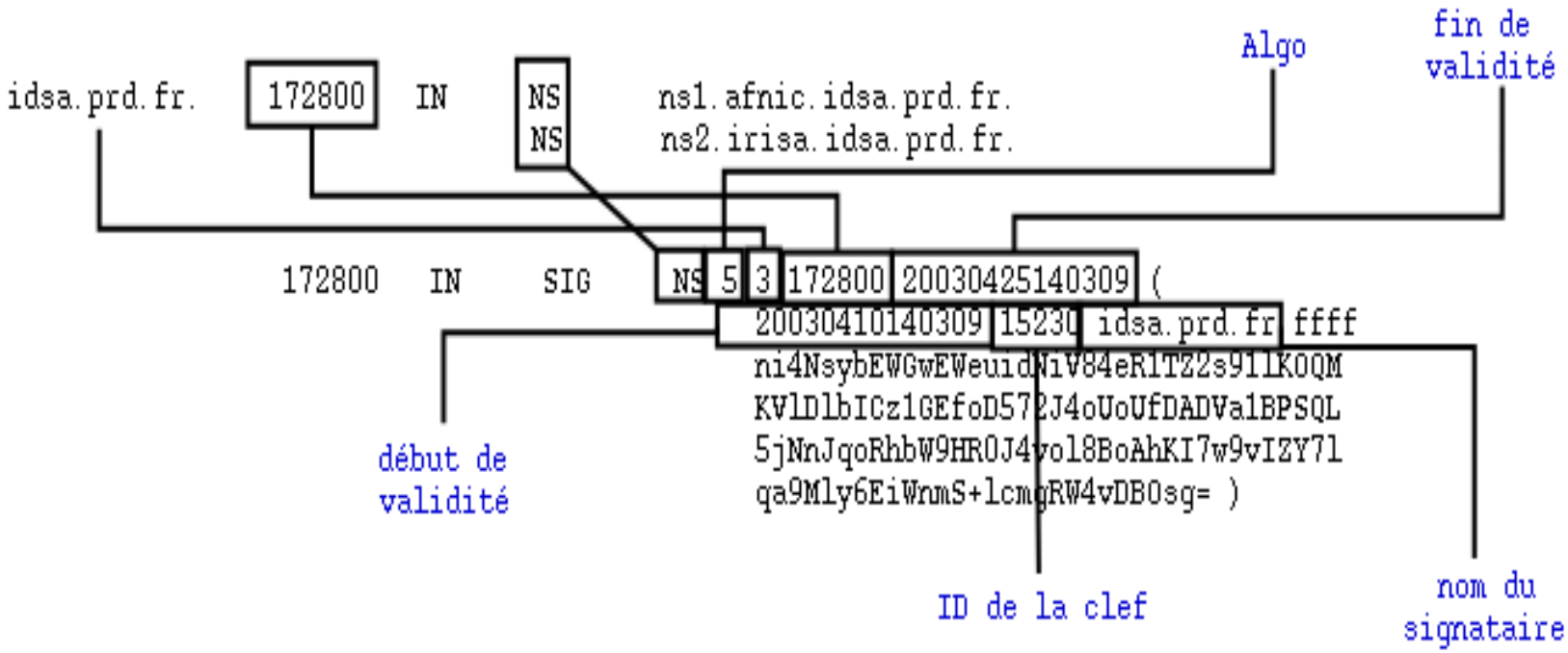
Nouveaux RRs

- Nécessité de stocker les objets utilisés par DNSsec au format RR
- KEY, SIG : sécuriser les RRsets
- NXT : garantir la complétude d'une zone
- DS : établir des chaînes de confiance

Format KEY: exemple



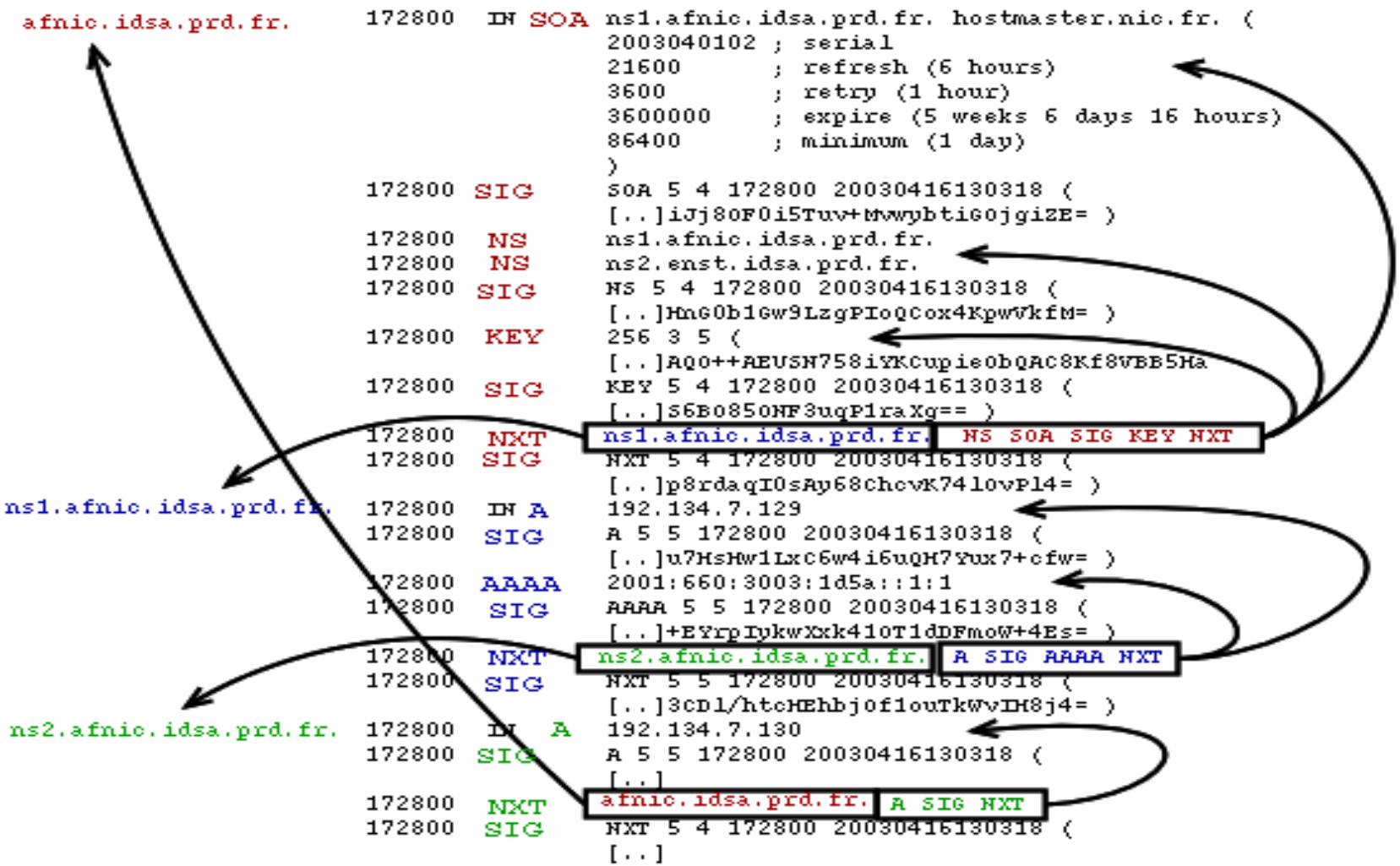
Format SIG: exemple



NXT: nécessité

- Comment signer les réponses négatives (authentification de la non-existence d'un nom ou enregistrement)
- Ordonnancement de la zone et insertion d'enregistrements NXT entre les noms.
- Le RR NXT d'un nom contient tous les types d'enregistrements associés à ce nom ainsi que le prochain nom présent dans la zone.

NXT: fonctionnement



NXT: pour aller plus loin

- Protection contre le rejeu et “déni de domaine”
- Attention : perte de confidentialité. Possibilité de récupérer tous les noms de la zone (DNS walk)
- Détection des Wildcards

Délégations sécurisées et chaînes de confiance : DS

- Modèle 2535/DS
- Transmission du keyset à la zone parent
- Génération du DS et signature de celui-ci dans la zone parent
- Dans la zone parent, pour tout point de délégation,
  - La présence d'un DS signé prouve l'existence d 'une délégation sécurisée et authentifie la clef associée au DS
  - L 'absence de DS, prouvée par le contenu du NXT prouve la non sécurité de la zone fille

Renommage des Enregistrements

- Protocole DNSsec en cours de réécriture :
  - Draft-ietf-dnsext-dnssec-protocol-03 (27/10/03)
  - Draft-ietf-dnsext-dnssec-records-05 (27/10/03)
- Nécessité de faire la distinction entre la RFC 2535 et la future version du protocole
- DNSKEY sera utilisé à la place de KEY et est strictement réservé au stockage des clefs DNSsec
- SIG à la place de RRSIG
- NXT à la place de NSEC
- DS reste DS puisqu'il n'existait pas dans la RFC 2535

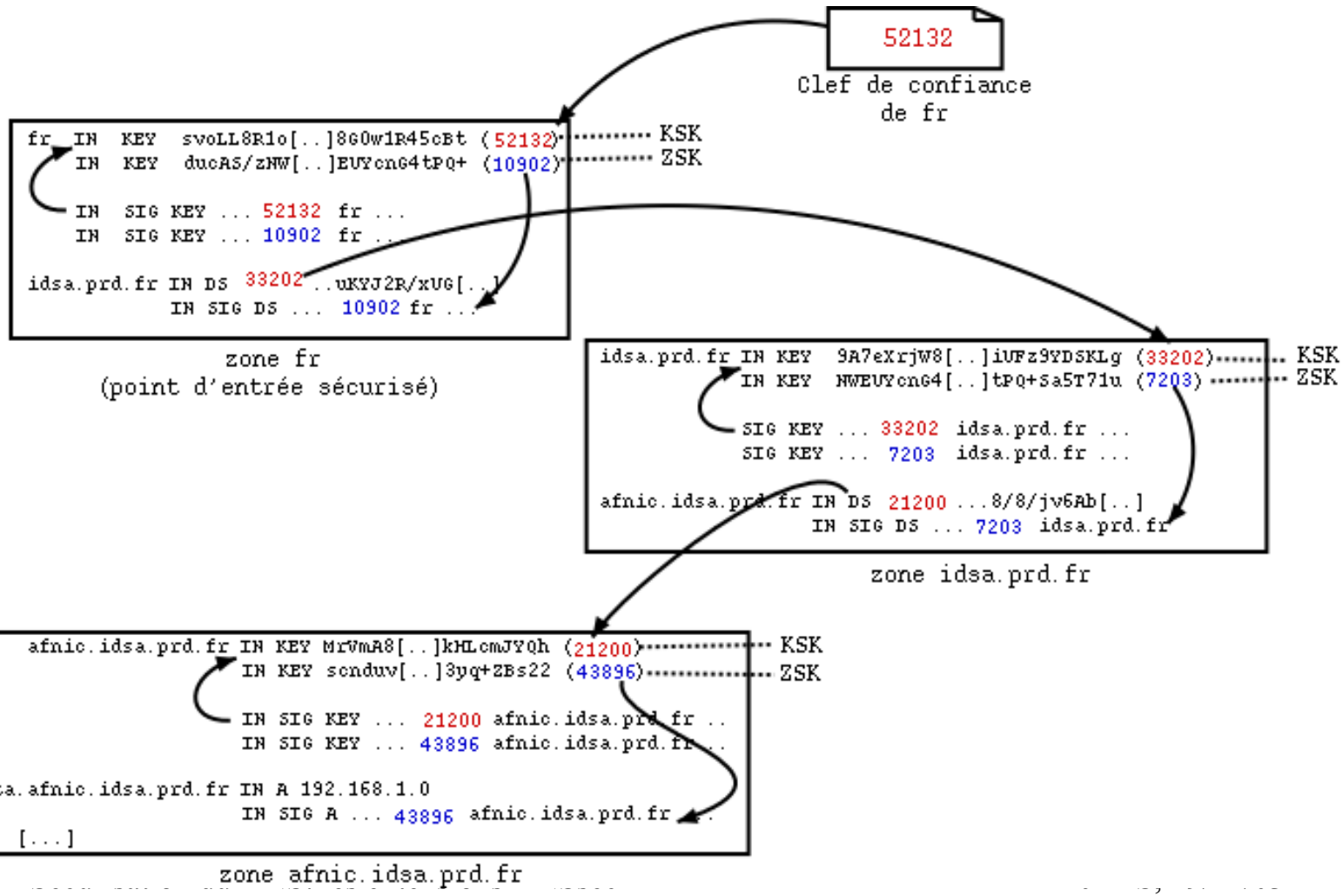
Importance d'un modèle à deux clefs

- Caractéristiques des clefs en fonction de leur taille :
- Clef courte :
  - Plus facile à casser
  - Temps de signature plus court
  - Temps de vérification des signatures par les utilisateurs plus court
  - Taille de zone réduite
- Clef longue :
  - Plus difficle à casser
  - Performances moins bonnes (signatures et vérifications)
- Les besoins DNSsec rendent le compromis difficile

Distinction ZSK/KSK

- Séparer les rôles :
  - Clef qui signe les enregistrements d'une zone: ZSK
  - Clef qui fait office de maillon de confiance: KSK. Elle ne signe que le KEY RRset
- Flexibilité accrue dans la relation zone parent/ zone fille

Authentifications en cascade dans une chaîne de confiance



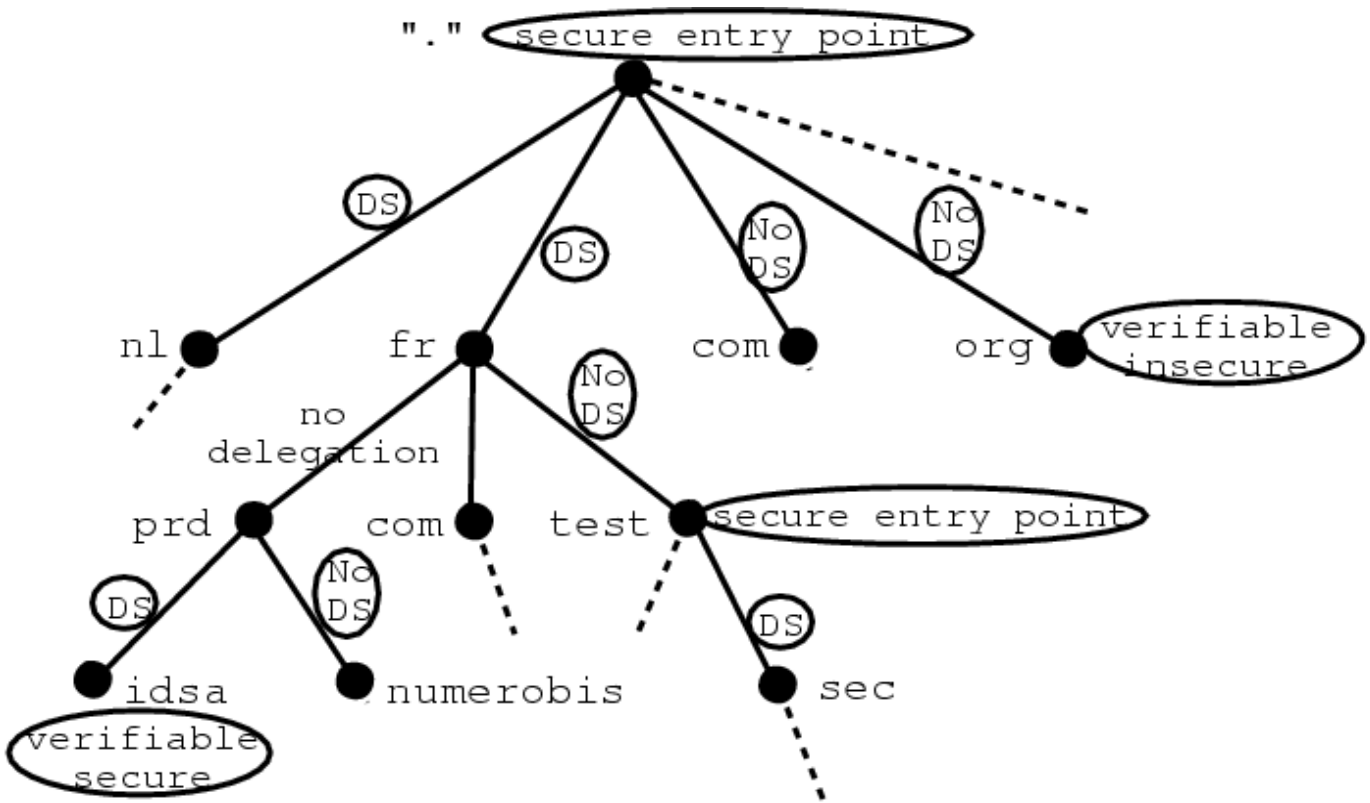
Classification des informations DNS (1)

- Classification objective
  - zone non sécurisée
  - sécurisée localement
  - sécurisée globalement
- Sécurisation progressive de l'arbre et îlots sécurisés

Classification des informations DNS (2)

- Classification subjective :
  - dépendante du resolver en fonctions des clefs de confiance dont il dispose
  - “verifiable secure”, “verifiable insecure”, “ wrong”
- Notions de point d’entrée sécurisé et clefs de confiance

Arbre DNS partiellement sécurisé



Roulement des clefs

- Possibilité de compromission des clefs
  - perte ou vol de la partie privée
  - attaques cryptanalytiques
- Efficacité du modèle ZSK/KSK
- Précautions concernant les temps caractéristiques (validité des sigs, intervalle de resignature, TTLs)

Roulement des clefs (2)

- Roulement ZSK prévu
  - considérations de TTLs, propagation dans les caches
- Roulement KSK prévu
  - transmission de la nouvelle KSK
  - ne pas rompre la chaîne de confiance
- Roulements d'urgence
  - nécessité d'une politique de sécurité locale

Sécurité des transactions: motivations

- Besoin de sécurité spécifique pour :
  - Le transfert de zones
  - Les mises à jour dynamiques (DNS Dynamic Updates)
  - Le dernier canal entre serveur récursif et client resolver (ou résolveur)
- Déployable indépendamment de DNSsec

Sécurité des transactions: TSIG

- Transaction SIGnature (RFC 2845) : meta RR
- Secret partagé (cryptographie symétrique)
- Signature d'un hash (algorithme HMAC-MD5)
- Authenticité et intégrité
- Protection contre le rejeu par "Timestamp" (synchronisation NTP nécessaire)

TSIG : utilisation pour un transfert de zone

- Générer une clef (dnssec-keygen)
- Transmettre cette clef secrète au serveur secondaire (hors-bande, PGP, scp, etc..)
- Configurer les serveurs

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 1

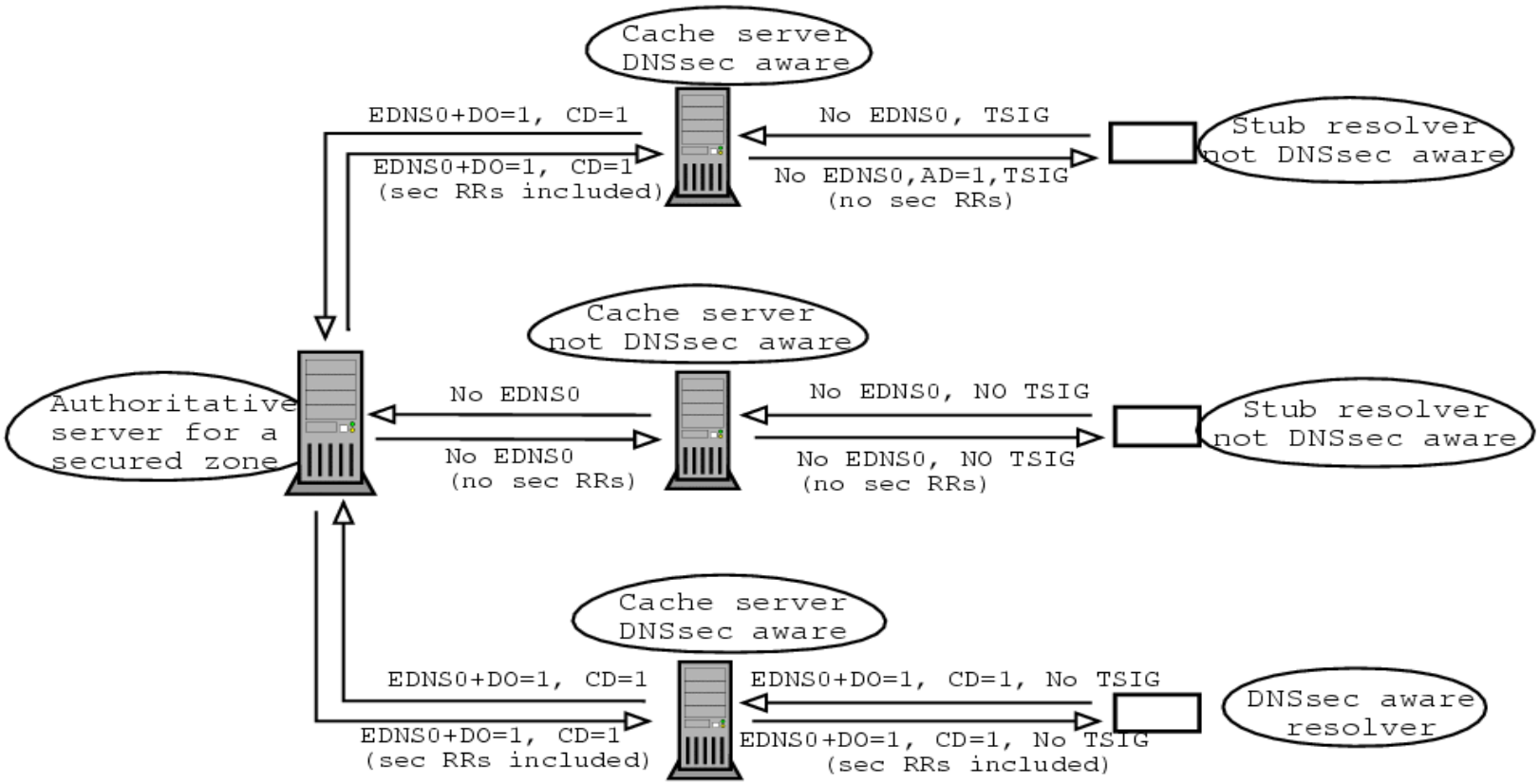
Une méthode à clefs publiques pour sécuriser les transactions : SIG(0)

- Très peu implémentée et utilisée
- Principalement pour les mises à jour dynamiques
- Utilise une clef publique stockée dans le DNS

Indication du support DNSsec

- Cohabitation entre entités supportant et ne supportant pas DNSsec
  - indiquer le support DNSsec
  - normaliser le comportement envers les données signées et les RRs de sécurité
- Les extensions EDNS0 (flag DO)
- Deux nouveaux flags : AD et CD

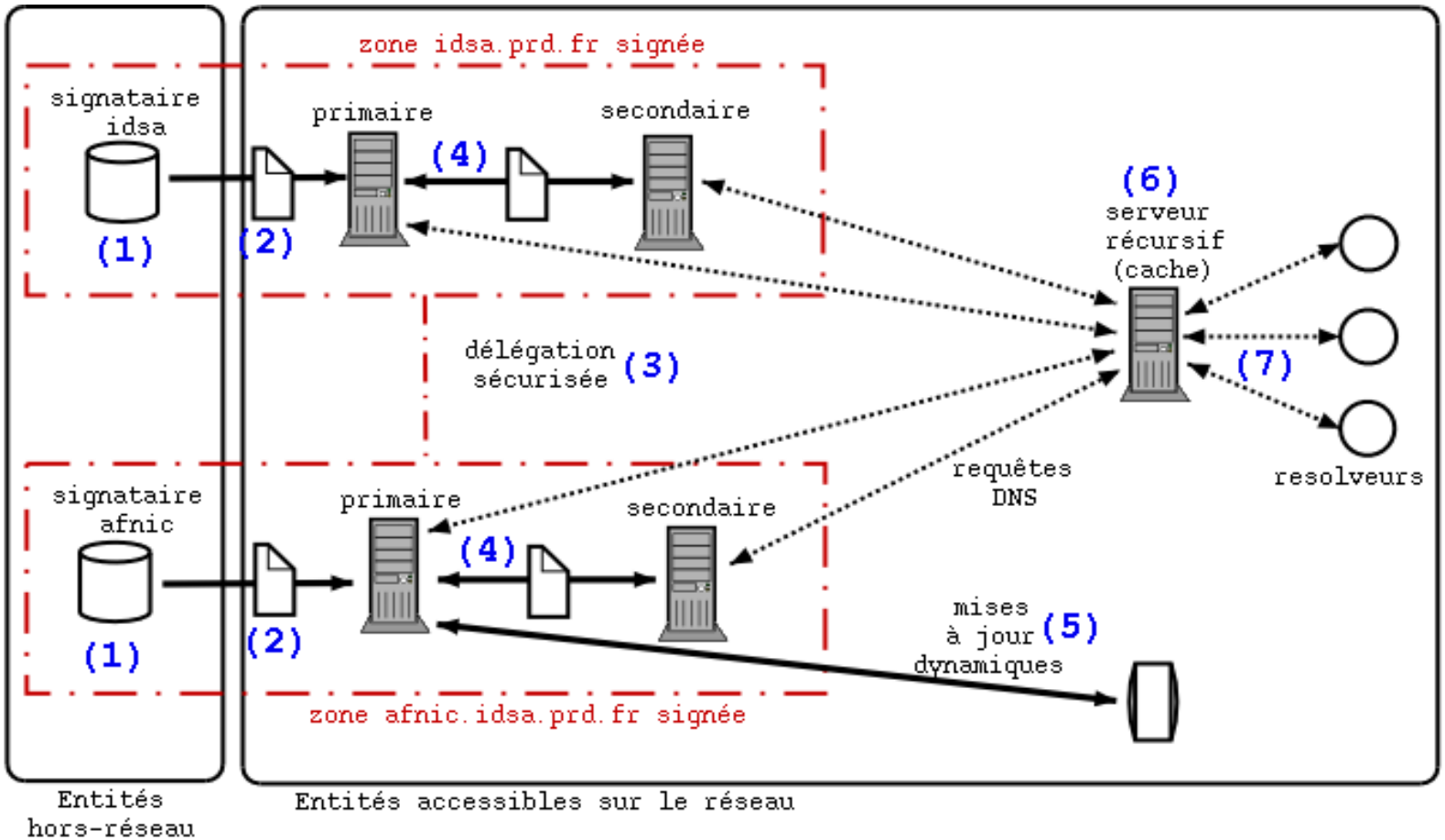
Scénarios de déploiement



Considérations opérationelles

- Utilisation de BIND9.3s (snapshots) et ses outils
- Performances
  - temps de signature
  - taille de la zone signée
- Nécessité d'un niveau de sécurité intrinsèque des serveurs
- Nouveaux enjeux : maintenance
  - automatisation des procédures
  - surveillance
  - responsablilité dans les chaînes de confiance
  - précautions pour la gestion des clefs

Bilan opérationnel



Expérimentations DNSsec

- Protocole toujours en évolution
- Expérimentations et retours d ’expérience assez limités
- Sécurisation de la zone fr (Autosign-TLD) sur des serveurs non référencés par les serveurs racine
- Projet RS.net: serveurs racine alternatifs et délégations sécurisées vers les TLDs participants: .fr, .nl, .se, .jp ...

Le projet IDsA

- Projet RNRT IDsA (Infrastructure DNSsec et Applications): *http://www.idsa.prd.fr et ftp://ftp.idsa.prd.fr*
- Déploiement d' une plate-forme de tests
- Développement d' outils de vérification des chaînes de confiance et d 'un resolver supportant DNSsec
- Développement d 'outils d 'automatisation des procédures
- Etude des interactions avec IPsec et Mobile IPv6

Conclusions

- DNSsec : sécurité contre les attaques spécifiques au DNS en proposant authentification de la source et intégrité des données
- Déployable dès maintenant et compatible avec le DNS non sécurisé mais protocole non encore finalisé
- Enjeux:
  - automatisation des procédures
  - résolveur supportant DNSsec
- Rôle de pseudo-PKI pour distribuer les clefs d ’autres applications

Références/ liens utiles

- http://www.idsa.prd.fr
  - bertrand.leonard@nic.fr
  - dnssec@nic.fr
  - idsa-tech@nic.fr
- http://www.isc.org
- http://www.ietf.org/html.charters/dnsext-charter.html
- http://www.dnssec.net

A propos de ce document

- **Auteur** : Bertrand Leonard
- **Copyright IDsA** :

Questions