DNSSEC

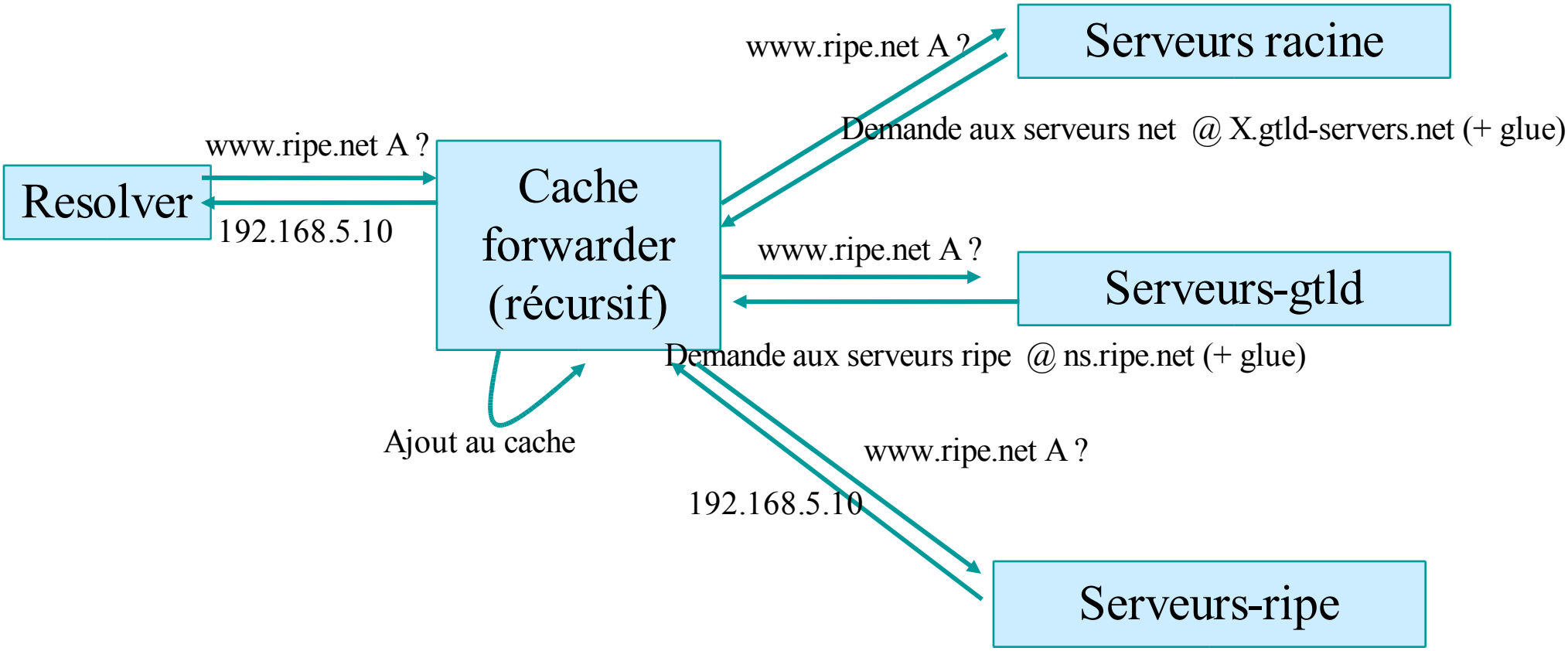
Alain Patrick AINA
aalain@trstech.net

Introduction
Quoi et pourquoi et ...

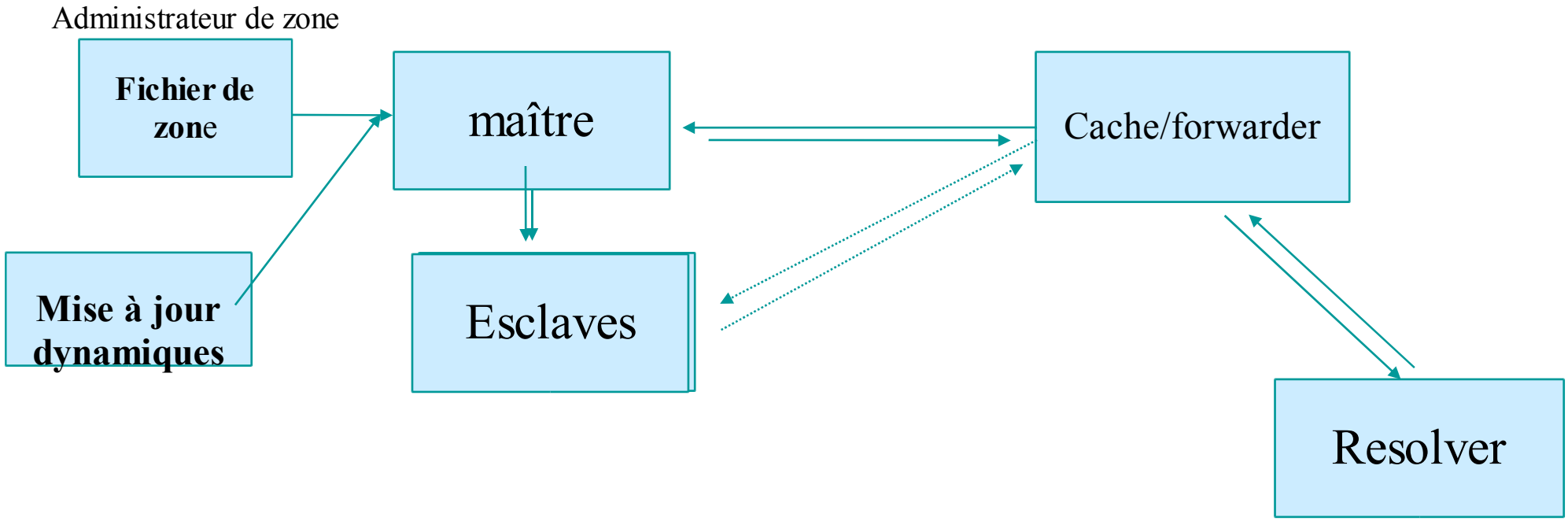
- QUOI:
  - DNS, DNSSEC et les derniers développements
- POURQUOI:
  - Informer sur DNSSEC
  - Fournir le nécessaire pour le démarrage du déploiement
- Pour:
  - Des personnes qui connaissent le DNS et veulent savoir plus sur DNSSEC

Résolution DNS

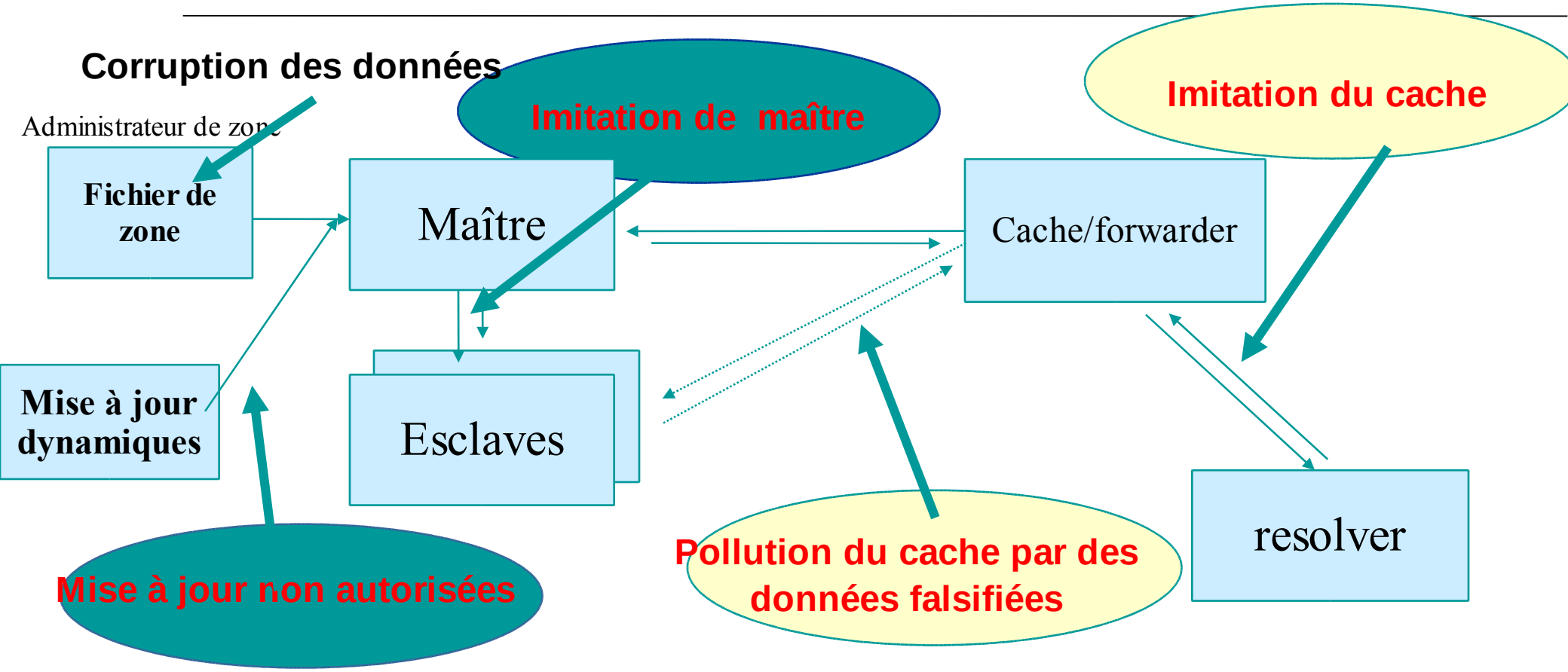
Question: www.ripe.net A



DNS
Mouvement des données



DNS
Vulnérabilités



Protection de serveur

Protection des données

Vulnérabilités du protocole DNS

- Les données DNS peuvent être falsifiées et corrompues sur leur chemin entre serveur et resolver ou forwarder
- Le protocole DNS ne permet pas la vérification de la validité des données DNS
  - Exploitation par des bugs dans des impléméntations de resolver (prévision de numéro de transaction)
  - Cache/forwarder pollué peut causer des dommages pendant un certain temps (TTL)
  - Des données DNS corrompues peuvent entrer en cache et y séjourner pendant longtemps
- Comment un esclave sait qu'il parle au bon maître ?

Pourquoi: Pour protéger le système DNS lui-même

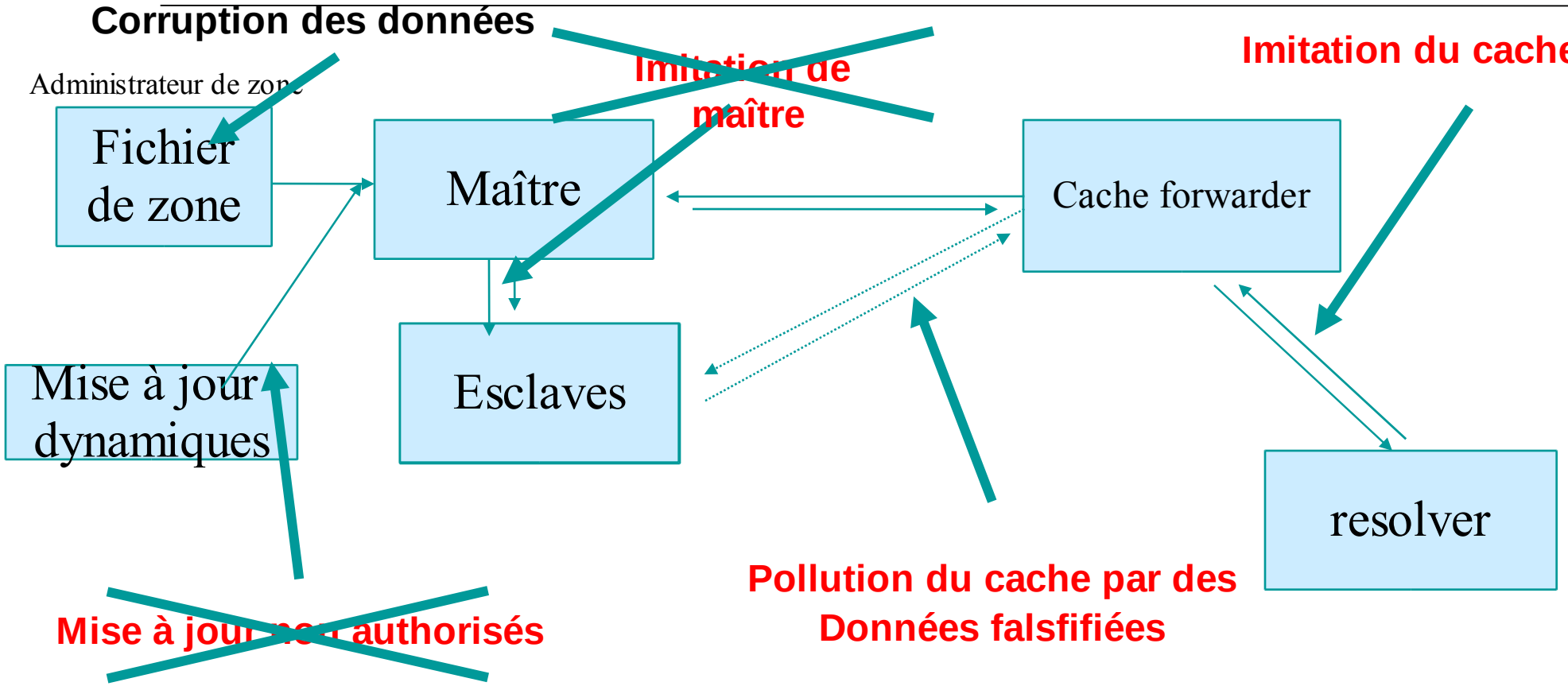
DNSSEC protège contre la corruption et la falsification des données

- DNSSEC donne aussi des mécanismes pour authentifier les serveurs
- DNSSEC donne des mécanismes pour établir l'authenticité et l'intégrité.

Un DNS sécurisé sera utilisé comme une ICP

- Même si cela n'a pas tous les attributs d'une ICP

Vulnérabilités protégées par TSIG



Mécanismes de DNSSEC Pour authentifier les serveurs

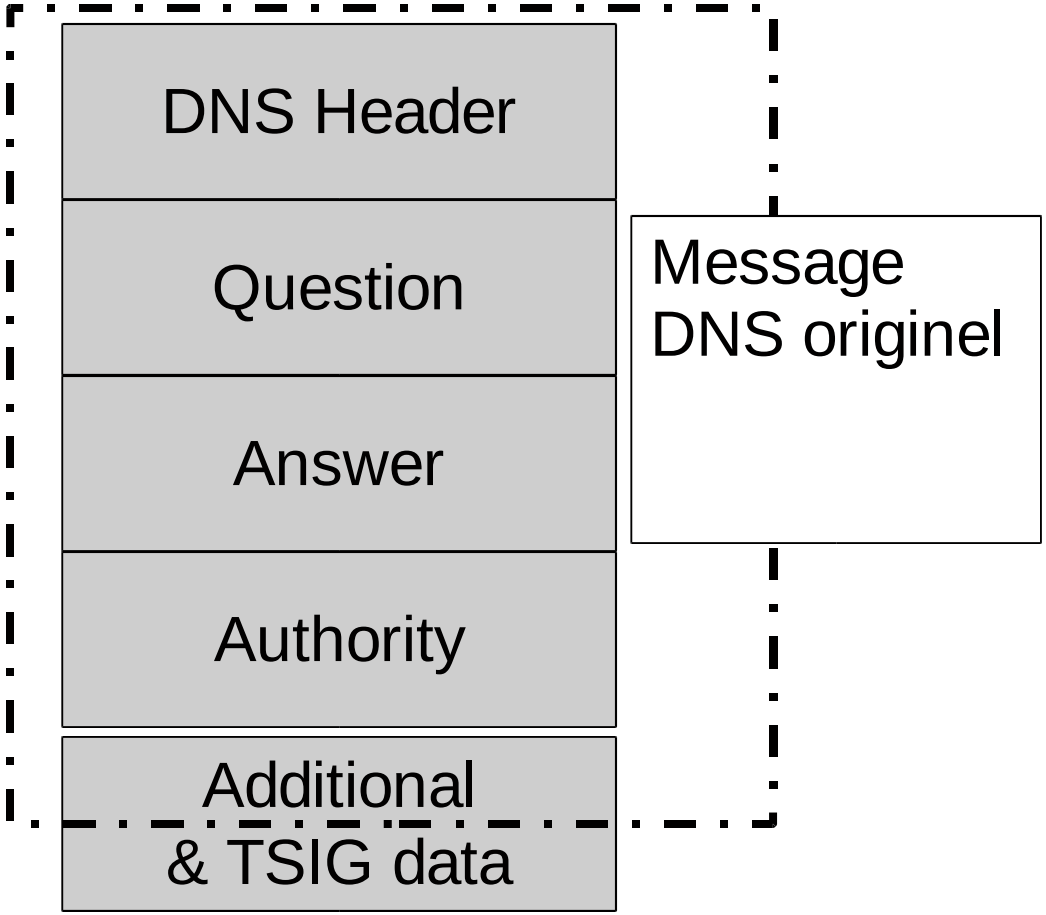
- Transaction Signature: TSIG (RFC 2845)
  - Autorisations des mises à jour dynamiques
  - Transferts de zone
  - Authentification de cache/forwarders
  - Peut être utilisée sans déployer d'autres données de DNSSEC
- Dans la configuration du serveur, non dans le fichier de zone
- Basée sur des valeurs secrètes partagées
  - Usage limité dû aux limitations de distribution de valeur secrète

Mécanismes de DNSSEC pour authentifier les serveurs (suite)

- Alternativement, l'on peut aussi utiliser SIG0
  - Pas encore généralement utilisé
  - Fontionne bien dans un environnement de mise à jours dynamiques
- Algorithme à clé publique
  - Authentification contre une clé publique publiée dans le DNS

- **TSIG/SIG0 signe une question/réponse d'un DNS avec un tampon de temps**
  - Synchronisation par NTP!!!

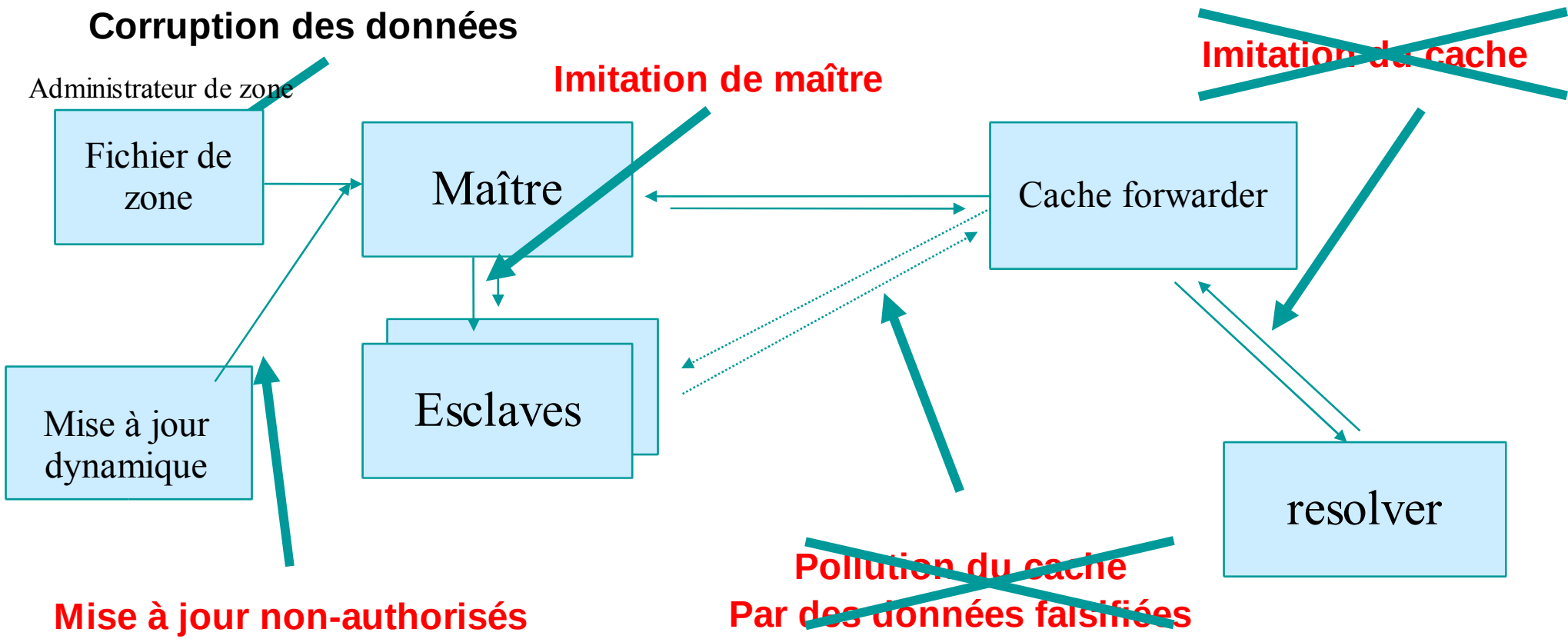
TSIG et format des messages



Noms et valeur sécrète

- Nom TSIG
  - Un nom est donné à la clé
  - Le nom est ce qui est transmis dans le message (Ainsi le récepteur sait quelle clé l'expéditeur a utilisé)
- Valeur secrète TSIG
  - Une valeur determinée durant la création de la clé
  - Généralement vue codée en Base64

Vulnérabilités couvertes par la protection des données



DNSSEC en une page

- Intégrité et authenticité des données avec la signature des enregistrements de ressources
- Des clés publiques peuvent être utilisées pour vérifier les signatures
- Les enfants signent leur zone avec leur clé privée. L'authenticité de leur clé est établie par une signature sur cette clé par leur parent.
- Dans le cas idéal, seule une clé publique a besoin d'être distribuée hors bande.

Authenticité et Intégrité

- Nous voulons vérifier l'authenticité et l'intégrité des données DNS
- Authenticité: Est ce la donnée publiée par l'entité supposée autoritaire ?
- Intégrité: Est ce la donnée reçue conforme à celle publiée ?
- La cryptographie à clé publique aide à répondre à ces questions
  - On peut utiliser les signatures pour vérifier l'intégrité et l'authenticité de donnée
  - On peut vérifier l'authenticité des signatures

Cryptographie à clé publique

- Deux clés disponibles: une clé privée et une clé publique
- Bref:
  - Si tu connais la clé publiqe, tu peux déchiffrer une donnée chiffrée avec la clé privée
    - Signature et vérification de signature
  - Si tu connais la clé privée, tu peux déchiffrer une donnée chiffrée avec la clé publique.
    - Confidentialité
- DNSSEC utilise seulement les signatures
  - PGP utilise les deux techniques

Cryptographie à clé publique (suite)

- La sécurité du système de cryptographie est basée sur un tas d'équations mathématiques dont la résolution demande le parcours d'un grand espace de solution (*e.g.* factorisation)
- Algorithmes : DSA, RSA, elliptic curve
- Les clés publiques ont besoin d'être distribuées. Les clés privées ont besoin d'être gardées secrètes
  - Pas evident
- La cryptographie à clé publique est 'lente'

Nouveaux “ER” DNSSEC

- 3 Enregistrements de Ressource à base de clé publique
  - RRSIG: Signature d'un “jeu” de ER faite avec la clé privée
  - DNSKEY: Clé publique, nécessaire pour la vérification d'un RRSIG
  - DS: Delegation Signer: ‘Pointeur’de construction de chaîne de confiance
- 1 ER pour la consistence interne
  - NSEC: ER pour indiquer le nom suivant dans la zone et quel type de ER sont disponibles pour le nom actuel
    - Authentifie la non existence de données
- Pour des clés publiques non DNSSEC : CERT/IPSECKEY(?)

ERs et “jeu” de ERs

- Enregistrement de ressource:
  - **label class ttl type rdata**

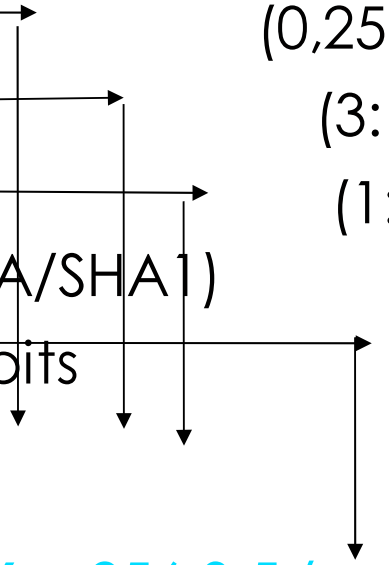
    www.ripe.net IN 7200 A 192.168.10.3
- Tout les ERs d’un “label” donné, “class”, “type” forment un “jeu” de ER:

  www.ripe.net IN 7200 A 192.168.10.3

  A 10.0.0.3
- Dans DNSSEC, ce sont les “jeux” de ER qui sont signés et non les ERs individuels

RDATA de DNSKEY

- 16 bits FLAGS (0,256,257)
- 8 bits protocole (3: DNSSEC)
- 8 bits algorithme (1: RSA/MD5, 2: DH, 3: DSA, 4: Elliptic curve, 5: RSA/SHA1)
- Clé publique à N*32 bits



Exemples:

ripe.net. 3600 IN **DNSKEY** 256 3 5 (
AQOvhvXXU61Pr8sCwELcqqq1g4JJ
CALG4C9EtraBKVd+vGIF/unwigfLOA
O3nHp/cgGrG6gJYe8OWKYNgq3kDChN)

RSA/SHA1 est recommandé maintenant

RDATA de RRSIG

- 16 bits type couvert
- 8 bits algorithme
- 8 bits labels couvert
- 32 bit TTL originel
- 32 bit expiration de signature
- 32 bit début de validité de signature
- 16 bit ID de clé
- Nom du signataire

```
www.ripe.net.   3600 IN  RRSIG   A 1 3 3600
20010504144523 (
                20010404144523 3112 ripe.net.
                VJ+8ijXvbrTLeoAiEk/qMrdudRnYZM1VlqhN
                vhYuAcYKe2X/jqYfMfjfSUrmhPo+0/GOZjW
                66DJubZPmNSYXw== )
```

RDATA de NSEC

- Nom suivant dans la zone
- Liste également les types de ER existants pour un nom
- L'enregistrement NSEC du dernier nom pointe vers le premier nom dans la zone
- Exemple:

www.ripe.net. 3600 IN **NSEC** ripe.net. A RRSIG NSEC

Enregistrement NSEC

- Authentification de la non-existence de “type” et de “labels”

  Exemple de la zone ripe.net (Sans les RRSIG):

```
@           SOA      .....
            NS   NS.ripe.net.
            DNSKEY .............
            NSEC     mailbox  DNSKEY   NS NSEC RRSIG SOA
mailbox             A     192.168.10.2
                    NSEC     www A NSEC RRSIG
WWW                 A     192.168.10.3
            NSEC      ripe.net  A NSEC RRSIG
```

dig smtp.ripe.net donnerait: **aa RCODE=NXDOMAIN**
autorité: mailbox.ripe.net. NSEC www.ripe.net. A NSEC RRSIG
dig www.ripe.net MX donnerait: **aa RCODE=NO ERROR**
autorité: www.ripe.net. NSEC ripe.net. A NSEC RRSIG

Delegation Signer: DS

- Indique que la zone déléguée est digitalement signée
- Essentiellement un pointeur vers la clé suivante dans la chaîne de confiance
- Le Parent est autoritaire pour le DS des zones enfant
- **Le DS ne doit pas être publié dans la zone enfant.**
- Règle beaucoup de problèmes
  - Renouvellement de clés

Delegation Signer: DS (suite)

- DS : Le parent donne l'autorité de signer les ERs du DNS à l'enfant en utilisant le DS
- Est un pointeur vers prochaine clé dans la chaîne de confiance
  - Tu fais confiance à une donnée qui est signée en utilisant une clé vers laquelle pointe le DS

RDATA du DS

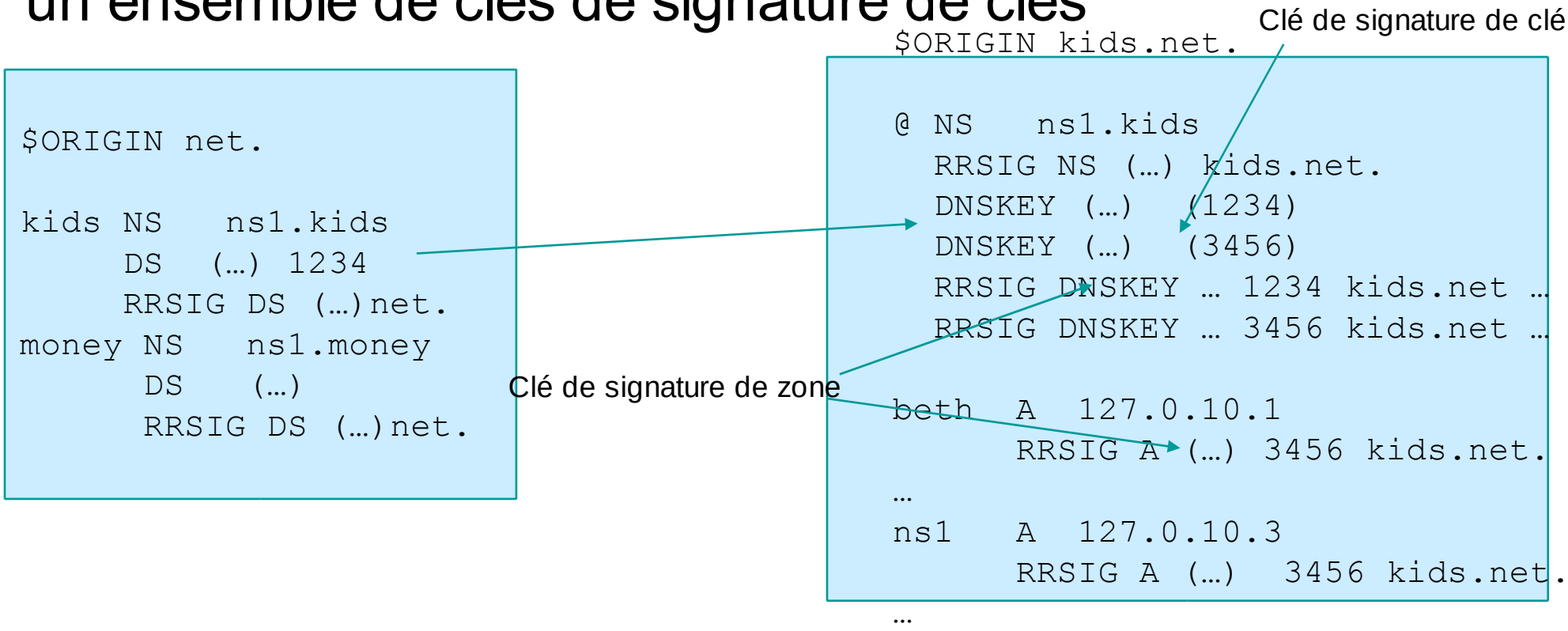
- 16 bits ID de la clé de l'enfant
- 8 bits algorithme
- 8 bits type de digest
- 20 octets de digest SHA-1

Ce champ indique la clé suivante dans la chaîne de confiance

```
$ORIGIN ripe.net.
disi.ripe.net     3600 IN   NS   ns.disi.ripe.net
disi.ripe.net.    3600 IN   DS   3112  5 1 (
                                  239af98b923c023371b52
                                  1g23b92da12f42162b1a9
                                  )
```

Délégation de zone signée

- Le Parent signe l'enrégistrement DS pointant vers un ensemble de clés de signature de clés



Clés de signature de clé/zone

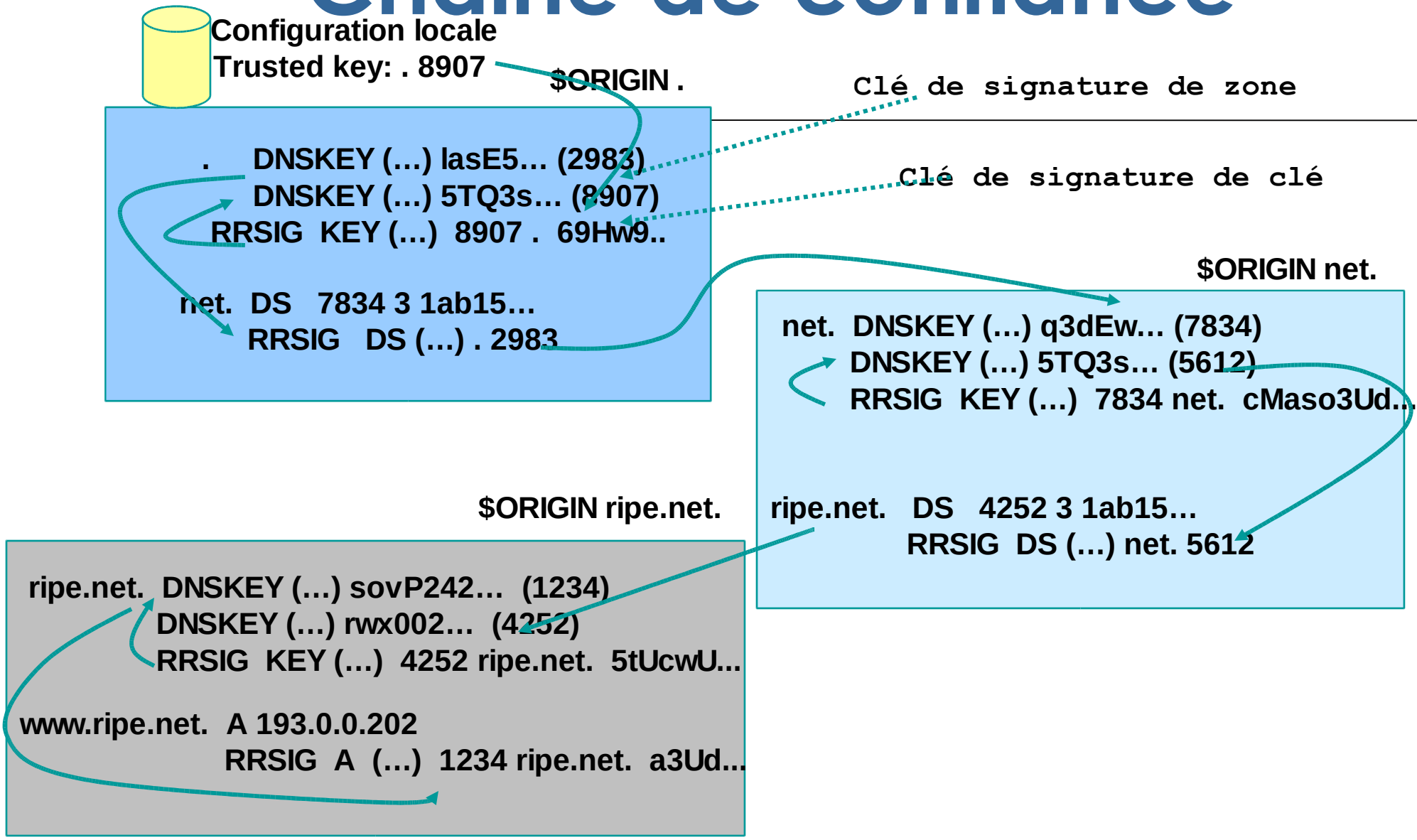
- DS pointe vers la clé de signature de clé (KSK)
- La zone est signée avec la clé de signature de zone(ZSK)

- KSK peut être plus grande avec une grande durée de vie
- ZSK peut avoir une durée de vie courte
  - Peut être “petit” = “rapidité”

Chaîne de confiance

- Les données dans les zones peuvent être valides si elles sont signées par une ZSK
- La ZSK ne peut être valide que si elle est signée par une KSK
- La KSK ne peut valide de foi que si elle référencée par un enregistrement DS de confiance
- Un enregistrement DS ne peut être valide que s'il est signé par la ZSK du parent ou
- Une KZK peut être valide si elle est échangée hors bande (Trusted key)

Chaîne de confiance



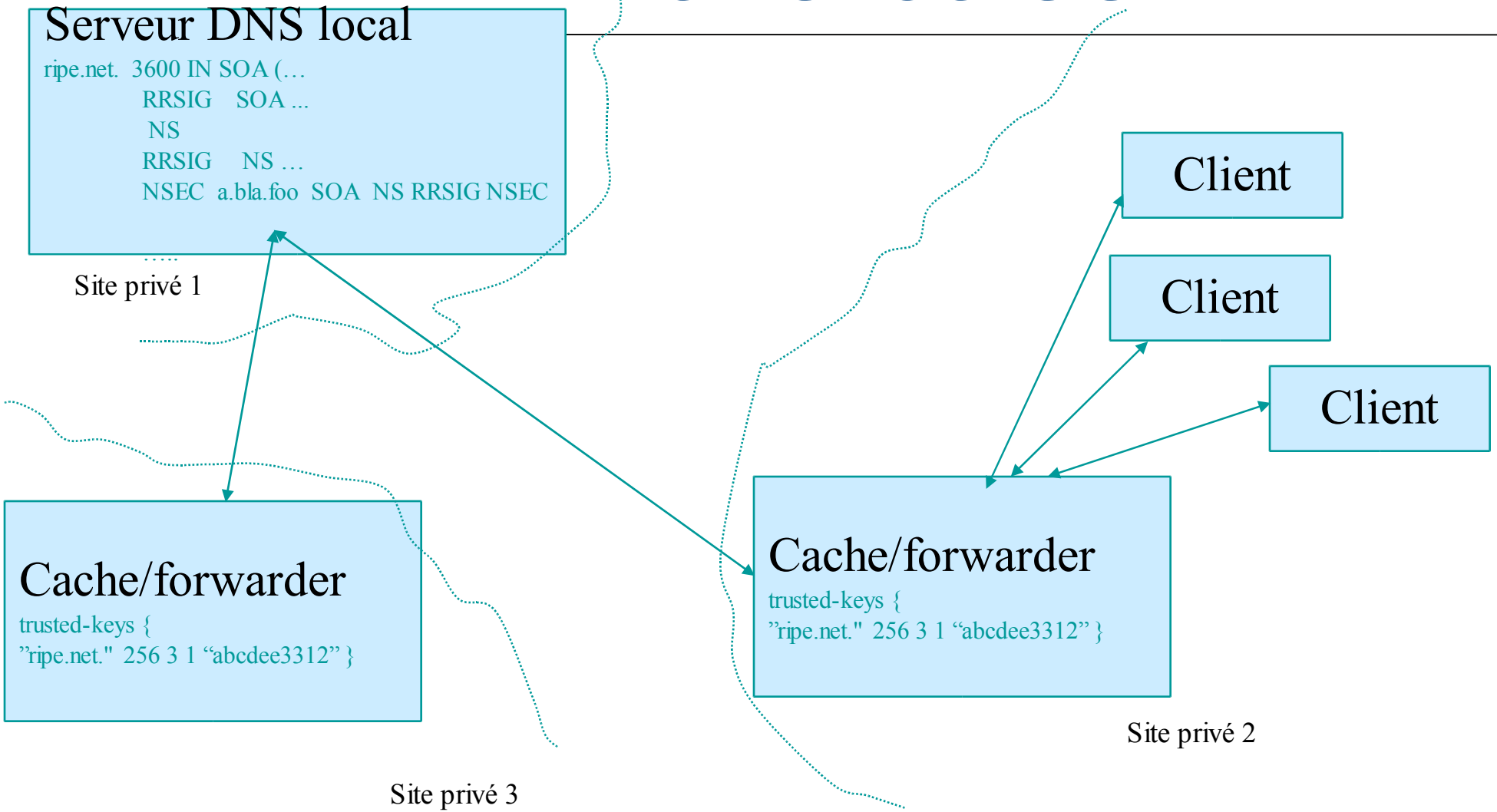
Signature DNSSEC d'une zone isolée

- 2 actions pour sécuriser une zone à utilisation interne
- Signer votre zone

  La signature va :
  - Trier la zone
  - Insérer les enregistrement NSEC
  - Insérer RRSIG contenant une signature pour chaque "jeu" d'enregistrement de ressource.

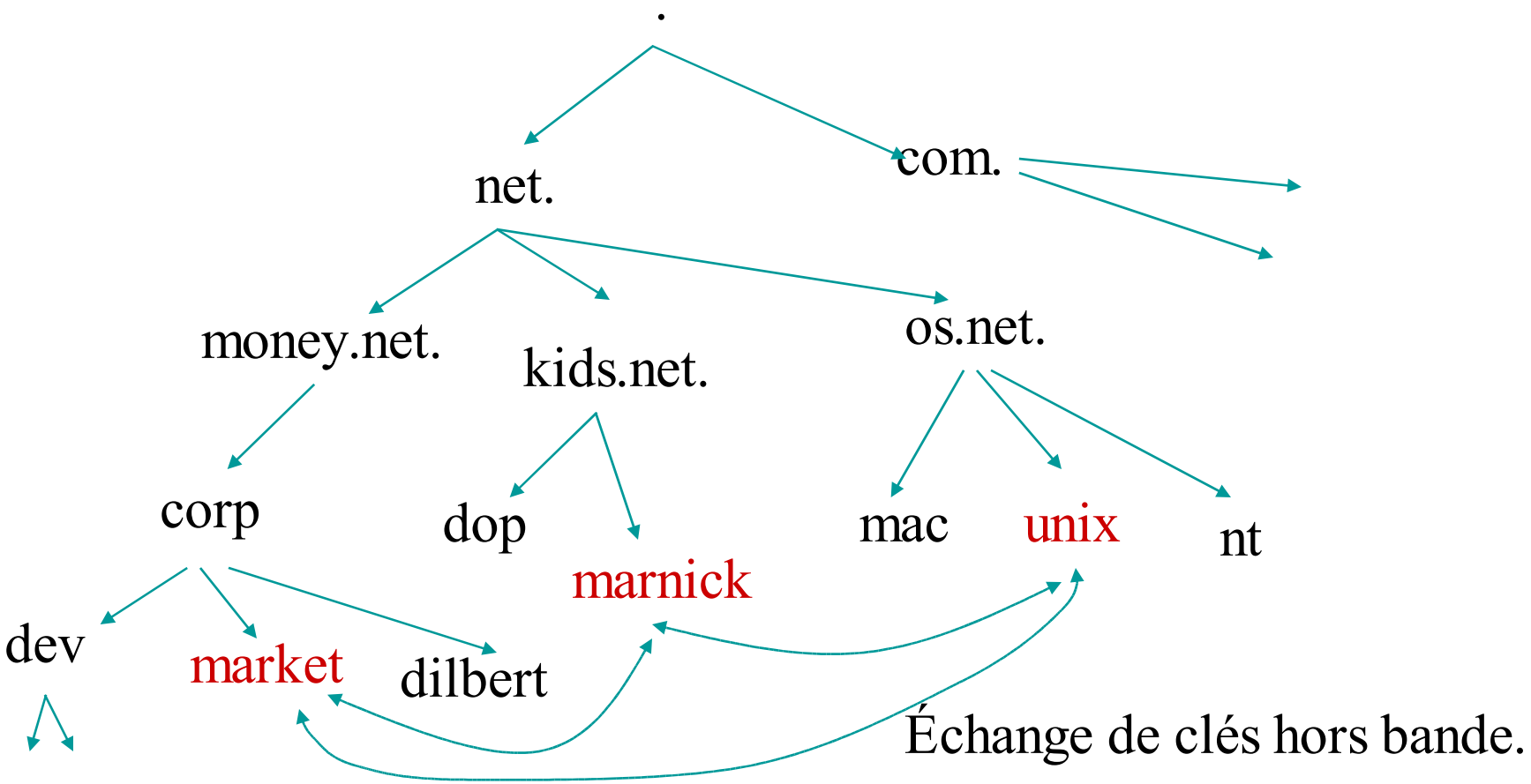
  La signature est faite avec votre clé privée
- Distribuer la clé publique à ceux qui veulent faire confiance à votre zone.
  - A configurer dans leur "resolver"

Signature DNSSEC d'une zone isolée



Sécurisation d'une arborescence du DNS

- Problème de distribution de clés



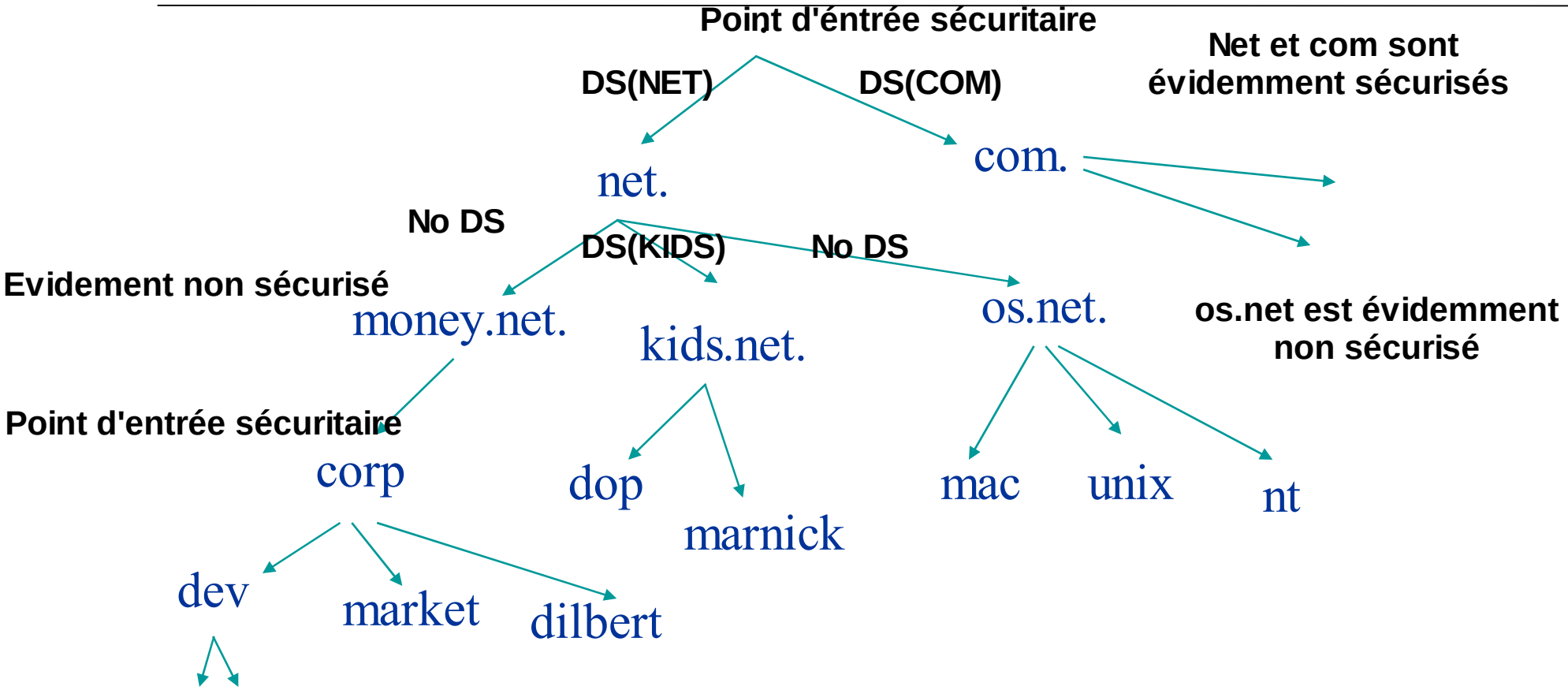
Utilisation du DNS pour distribuer les clés

- Construction des chaînes de confiance de la racine vers le bas de l'aborescence DNS
  - Outils:
    - ERs: CLES, RRSSIG, DS, NSEC
    - Configuration manuelle des clés de la racine

Des zones non sécurisées

- L'évidence cryptographique de l'état non sécurisé d'une zone est fournie par le parent
- S'il n'y a pas d'enregistrement DS, comme prouvé par un enregistrement NSEC avec une signature valide, l'enfant n'est pas sécurisé.
- Un enfant peut contenir des signatures,mais celles-ci ne seront pas utilisées pour construire une chaîne de confiance

Lexique (RFC3090)



Resolver a les clés de la racine et de corp.money.net configurées comme des points d'entrée sécuritaires

Pourquoi échanger et renouveller les clés?

- Vous devez garder votre clé privée secrète
- La clé privée peut être volée
  - Mettre la clé sur une machine isolée derrière pare-feu et un contrôle d'accès solide
- Reconstruction de clé privée (Analyse de cryptographie)
  - Nombre aléatoire pas vraiment aléatoire
  - Attaques brutales

Pourquoi échanger et renouveller les clés?(suite)

- Minimiser l'impact de la compromission de la clé privée
  - Courte validité des signatures
  - Renouvellement régulier de clés

- NB: Les clés n'ont pas de tempons horaires en elles; Les RRSIG sur les clés ont de temps horaire

Courte validité de signature

- Courte durée de signature du parent sur le ER DS protège l'enfant
- 1 jour possible

```
www.ripe.net.   3600 IN  RRSIG   A 1 3 3600 20010504144523 (
                20010404144523 3112 ripe.net.
                VJ+8ijXvbrTLeoAiEk/qMrdudRnYZM1VlqhN
                vhYuAcYKe2X/jqYfMfjfSUrmhPo+0/GOZjW
                66DJubZPmNSYXw== )
```

Signature expiration

Renouvellement de clés

- Avec la distinction de ZSK du KSK, il est maintenant possible de remplacer le ZSK sans affecter le parent
  - Il suffit seulement de re-signer le « jeu » ER du DNSKEY avec le KSK inchangé.
- Ceci est une forme de renouvellement de clé
  - On peut aussi remplacer le KSK
- Il est nécessaire d'avoir temporairement les deux clés (ancienne et nouvelle) présentes dans la zone
  - Assurer la transition
  - Jusqu'à expiration des RRSIG générées par l'ancienne clé

Bit AD

- Un bit d'état dans la section « header » des paquets DNS
  - Non utilisé avant DNSSEC(devrait être à zéro)
  - Utilisé uniquement dans les réponses d'un serveur de validation
  - Le bit AD n'est pas positionner par un serveur autoritaire.
- AD = Authenticated data(donnée authentifiée)
  - 1= signature de réponse vérifiée avec succès
  - 0= échec de vérification de signature de réponse

Bit CD

- Un bit d'état dans la section « header » des paquets DNS
  - Non utilisé avant DNSSEC(devrait être à zéro)
  - Utilisé uniquement dans les requêtes
- CD = Checking Disable (vérification désactivée)
  - 1= vérification désactivée
    - Le “resolver” accepte des réponses non vérifiées
  - 0= vérification activée
    - Le “resolver” veut des réponses vérifiées pour les données signées,mais accepte les réponses non vérifiées pour les données non signées

Bit DO

- Un bit d'état dans la section « header » des paquets DNS
  - Non utilisé avant DNSSEC (devrait être à zéro)
  - Utilisé uniquement dans les requêtes
  - 1= le “resolver” veut les enregistrements DNSSEC
  - 0= le “resolver” ne veut pas les enegistrements DNSSEC

Faiblesses du DNSSEC

- Ne protége pas contre les attaques de déni de service; mais en augmente les risques
  - Charge de travail de cryptographique
  - Longueur des message DNS
- Ne protège pas les ERs non signés(données non autoritaires aux points de délégation)
  - NS et glue dans la zone parent
  - Il faut protéger les transferts de zone par autres techniques
- Ajoute de la complexité au DNS, augmentant ainsi les risques de mauvaises configurations
- DNSSEC introduit un mécanisme qui permet de lister tous les noms d'une zone en suivant la chaîne NSEC

Faiblesses du DNSSEC

- DNSSEC crée un besoin de synchronisation de temps entre le client et l'entité créatrice des signatures DNSSEC
- Le renouvellement des clés au niveau de la racine est très difficile
  - Les travaux à ce jour n'ont pas déterminé comme ceci pourrait se faire, et même comme elles sont configurés en première place
- Comme le DNS, la chaîne de confiance du DNSSEC est hiérarchisée
  - Problème de dysfonctionnement dans la hiérarchie

Mise en oeuvre du DNSSEC

- BIND9
  - BIND 9.3.1
  - http//www.isc.org
- Librairies OPENSSL
  - http://www.openssl.org
- NTP
  - Ntpdate -b
  - xntpd

Exemples de TSIG

- **<<>> DiG 9.3.0 <<>> @localhost localhost a -k /var/named/Khost1-host2.+157+50032.key**
- ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18286
- ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
- ;; QUESTION SECTION:
- ;localhost. IN A
- ;; ANSWER SECTION:
- localhost. 86400 IN A 127.0.0.1
- ;; AUTHORITY SECTION:
- localhost. 86400 IN NS localhost.
- **;; TSIG PSEUDOSECTION:**
- **host1-host2. 0 ANY TSIG hmac-md5.sig-alg.reg.int. 1125416965 300 16 GDjgw1/mSX1z1+tAreB7Nw== 18286 NOERROR 0**
- ;; Query time: 4 msec
- ;; SERVER: 127.0.0.1#53(localhost)

Exemples de zone à signer

```
$TTL    86400
$ORIGIN localhost.
@               1D IN SOA       @ root (
                                46              ; serial (d. adams)
                                3H              ; refresh
                                15M             ; retry
                                1W              ; expiry
                                1h )            ; nttl
                        1D IN NS        @
                        1D IN A         127.0.0.1
                        1D IN AAAA      ::1
aalain                  A           127.0.0.3
bill                    MX      10 manning.ep.net.
                        MX      20 aalain.trtsech.net.
yaounde                 NS      ns.trstech.net.
yaounde                 NS      yaounde.cm.
```

Exemples de zone signée

```
localhost.          86400   IN SOA  localhost. root.localhost. (
                                    46          ; serial
                                    10800       ; refresh (3 hours)
                                    900         ; retry (15 minutes)
                                    604800      ; expire (1 week)
                                    3600        ; minimum (1 hour)   )
                    86400   RRSIG   SOA 5 1 86400 20041216222525 (
                                    20041215222525 37835 localhost.
                                    fDp6T3McTZBUPvN72wNrQXBF7pxsndyDOU6i
                                    YSJA/PVgo8dN8ytb+yvnHUEf5xRHrDTyDSII
                                    ZrX7UE9yaux6NxoVaAdtknsa2TNzeONz+h4r
                                    BPoaLHuH5L+EgZcjzS7U )
                    86400   NS      localhost.
                    86400   RRSIG   NS 5 1 86400 20041216222525 (
                                    20041215222525 37835 localhost.
                                    QTzH5qTrzF8wuFAkxJ2DBf7WLHZuoUdTlmlH
                                    Y+fxqeO4xVgRxktMxkNo6Fo4vig+QEhYjR0V
                                    8ugidrpRcWfeYxqcRbLm+Np/+giW+Bjjy3UJ
                                    5QgT3M2Z0NOJ2vikgrWp )
```

Exemples de zone signée (suite)

```
86400   A       127.0.0.1
        86400   RRSIG   A 5 1 86400 20041216222525 (
                20041215222525 37835 localhost.
                cX9T/cCJGr2Gr5Oz4G6kIZqL3ENyl90jgrQM
                exzl9luNX02IUBx6OZY4rGnSfW+ZybzOR78l
                Nu4fzARgQLqRHpp0hMd7DoDx9JmCDrZCzyXl
                Jxb5nhp6PrPOryAND8gn )
        3600    NSEC    aalain.localhost. A NS SOA RRSIG NSEC DNSKEY
        3600    RRSIG   NSEC 5 1 3600 20041216222525 (
                20041215222525 37835 localhost.
                GH+Gp3WuXscQFUgnoBntNMF8TQuiRAcpWvyg
                N984K1FGMjMzihVF93TfuTV9gkqs/+yE82ld
                RJsdK67lMLX15r7wpqLCKzGv97EUXrWPC71W
                HvYIHOX8r6qp8lzlyRiM )
```

Exemples de zone signée (suite)

```
86400   DNSKEY  256 3 5 (
            AQPFpBnSA70OstJ4Kw/Aj2pO8Kn6nKjNP7SF
            WEYzL1fzsNseBAObfG/SCIBs8xe7Az29Vdii
            ITNVf5FZHr4UFq2+SW0LEGXft1EBEYt85fN3
            PmYqoAxBY/MyOJMipSzNmmU=
            ) ; key id = 37835
86400   DNSKEY  257 3 5 (
            AQOw7JyQptn4Lp2gGZ7TMW1P0qPXo+QcpHhO
            ZcGO7xixfgS3w2g9D9+eltq70bh5bz2k+qx/
            WZj2kOA9AmrsIZCaQuPnA0cyuHK44S7QPms4
            FznG2bfxICMq8Uydlj4/1FM=
            ) ; key id = 32241
```

Exemples de zone signée (suite)

```
86400   RRSIG   DNSKEY 5 1 86400 20041216222525 (
                        20041215222525 32241 localhost.
                        pszwiFSueXJQf+K1Ot7lRzdhTBSFYohvTXc2
                        DDtHzHr6mHpOYFO+BhwBsFG1xAXbjzXZt1F5
                        MdjU7FnUYFbhPdSVWGIDjKubq74Ds2C0XfKk
                        ZU52Oy6VjQ2FaVCOSyO6 )
                86400   RRSIG   DNSKEY 5 1 86400 20041216222525 (
                        20041215222525 37835 localhost.
                        vWnwKo/RX/+edjxHeZswLW7LMBG8RyFKXM83
                        V7/hp49XvILrsLMPJx+qn3jczL2LzVQNokrT
                        DaTW0l2GVGe1I04nuTiQpRgtI8Gjzb3TXTTX
                        ugoz00fOReO4C4GZp0IJ )
aalain.localhost.       86400   IN A    127.0.0.3
```

Exemples de zone signée (suite)

```
86400   RRSIG   A 5 2 86400 20041216222525 (
                    20041215222525 37835 localhost.
                    BR/baHvQtUxl75pYTaOtdI/N/O4n20rrqCPt
                    8QWqyVtQFch/abP/BM9Sn0MVuIgKeqm01DKK
                    ZZrh34MYzcKg5W7nhij5WtmV1bcxEtlXsZJL
                    cwZF1qLC/msol8KRqpPC )
        3600    NSEC    bill.localhost. A RRSIG NSEC
        3600    RRSIG   NSEC 5 2 3600 20041216222525 (
                    20041215222525 37835 localhost.
                    jdgALAJa/DGIb2eZat89JY77Ab9kLHW2617X
                    orzXVDHl2OQbgXw+hocz2+8P2ifzbOgPWKLg
                    MVYkJ9WDTknOw1pR3aweVRbl4pRgSO/HY+hr
                    TzMAFZB4LMgXOBr+rSOR )
```

Exemples de zone signée (suite)

```
bill.localhost.      86400   IN MX   10 manning.ep.net.
                     86400   IN MX   20 aalain.trtsech.net.
                     86400   RRSIG   MX 5 2 86400 20041216222525 (
                                 20041215222525 37835 localhost.
                                 WChm4gACfrw5SMTTpPUfdtliNnm/u2jePS/4
                                 V9+wn/sqJ7dviMSGGLBjHeBcMtvQg6UZ+kSj
                                 py2ZF/GW7oP5FLxq7Vb4rYmLoosq78eevi0/
                                 ALhhPtZ2Q7H5HM+oG/vc )
                     3600    NSEC    yaounde.localhost. MX RRSIG NSEC
                     3600    RRSIG   NSEC 5 2 3600 20041216222525 (
                                 20041215222525 37835 localhost.
                                 ITI87dBSR5J7pESofHNn5THHIV5Lf9crzBPh
                                 lV7sNVbGr/6BP9axqauGkC0Kb3P7xKS2yGw0
                                 Hezef0qbZqKatBmVx0t0zqUK9tyF7SwG6MEK
                                 kyeXeEneewNpCsiSgd6k )
```

Exemples de zone signée (fin)

```
yaounde.localhost.      86400   IN NS   ns.trstech.net.
                        86400   IN NS   yaounde.cm.
                        3600    NSEC    localhost. NS RRSIG NSEC
                        3600    RRSIG   NSEC 5 2 3600 20041216222525 (
                                20041215222525 37835 localhost.
                                URLkUNy4kSQ/x/Qsp3WhoTv/jYFUusyWTSfo
                                6T1cy7a/XjqefB8t8jKsiBHuNwBqTpQCZ5PE
                                FEw2i0hMQpYOyiAl2I9oKWAzhKcnrhJWoS9e
                                BN11tshWn4AkFyxk0bvb )
```

Lectures

- http://www.bind9.net/manuals
- http://www.dnssec.net
- RFC(http://www.rfc-editor.org)
  - RFC 3833 (Vulnérabilités du DNS)
  - RFC 4033
  - RFC 4034
  - RFC4035

QUESTIONS ???