Introduction à DNSSEC

Alain Patrick AINA
aalain@trstech.net

Pourquoi DNSSEC

- Une bonne sécurité est multicouche
  - De multiples cycles de défenses physiques des systèmes sécurisés
  - Couches multiples dans le monde de gestion des réseaux
- Infrastructure DNS
  - DNSSEC pour constituer une barrière contre les attaques basées sur le DNS.
  - Fournit un anneau de sécurité autour de plusieurs systèmes et applications

Le Problème

- Les données DNS publiées sont remplacées en transit entre serveurs et clients.
- Ceci peut se produire à plusieurs endroits dans l'architecture DNS
  - **DNS utilise UDP, beaucoup plus facile à falsifier**
  - **Certains endroits sont plus vulnérables que d'autres**
  - **Les vulnérabilités dans les logiciels DNS facilitent les attaques (et il y aura toujours de vulnérabilités de logiciel)**
- Carences dans le protocole DNS et dans les déploiements classiques créent quelques faiblesses.
  - **Le Query ID est de 16 bits (0-65535)**
  - **Manque de randomisation de port source (16 bits) et de Query ID de paquets UDP dans certains déploiements**.

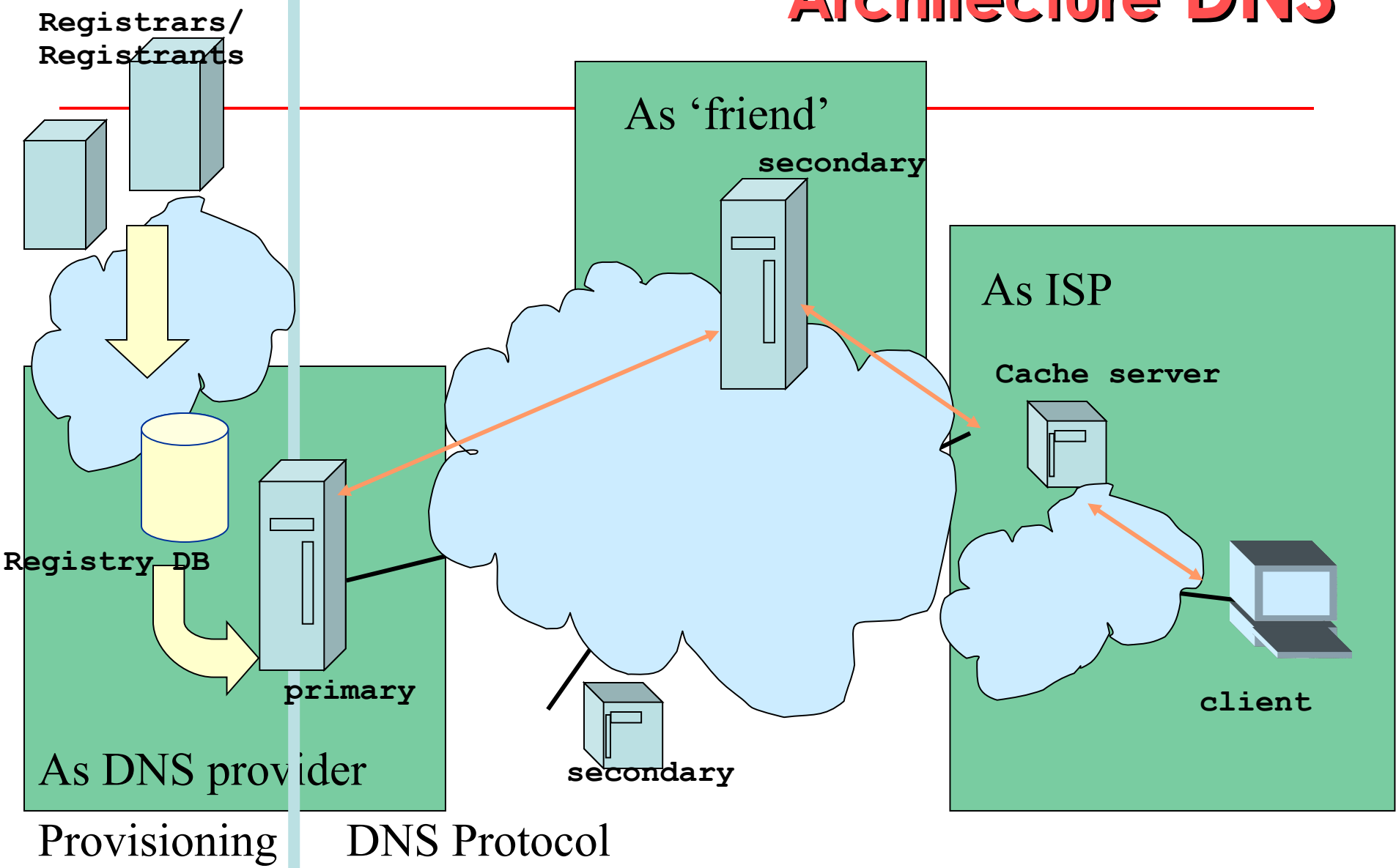
Le Problème(suite)

- Les attaques de Kaminsky publiées en 07/2008 ont montré comment ces faiblesses peuvent être exploitées pour des attaques de pollution de cache
  - Panique (bien que tout cela soit connu depuis!!!)
  - Contournements pour contenir la situation
    - **Randomisation de port source/Query ID**
    - **Recommandations pour le déploiement DNS**

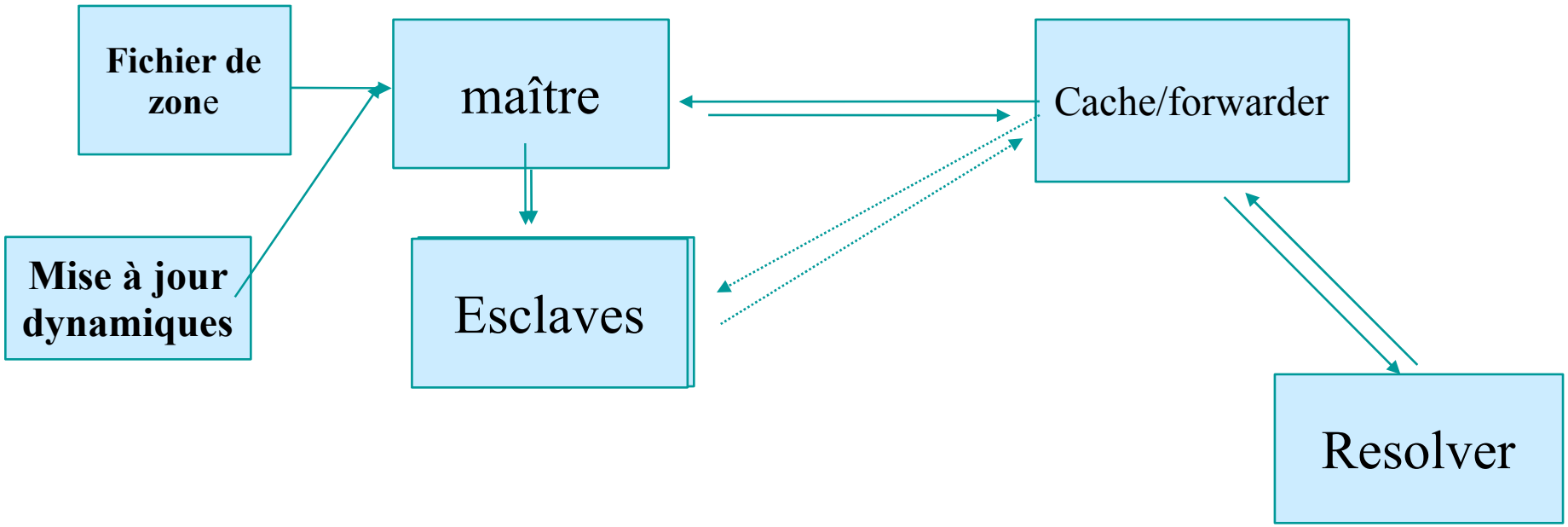
      http://www.kb.cert.org/vuls/id/800113
  - La Solution ????
    - **DNSSEC**

혼 **Et ainsi, DNSSEC est désormais connu comme un élément critique de la sécurité du DNS**.

Architecture DNS

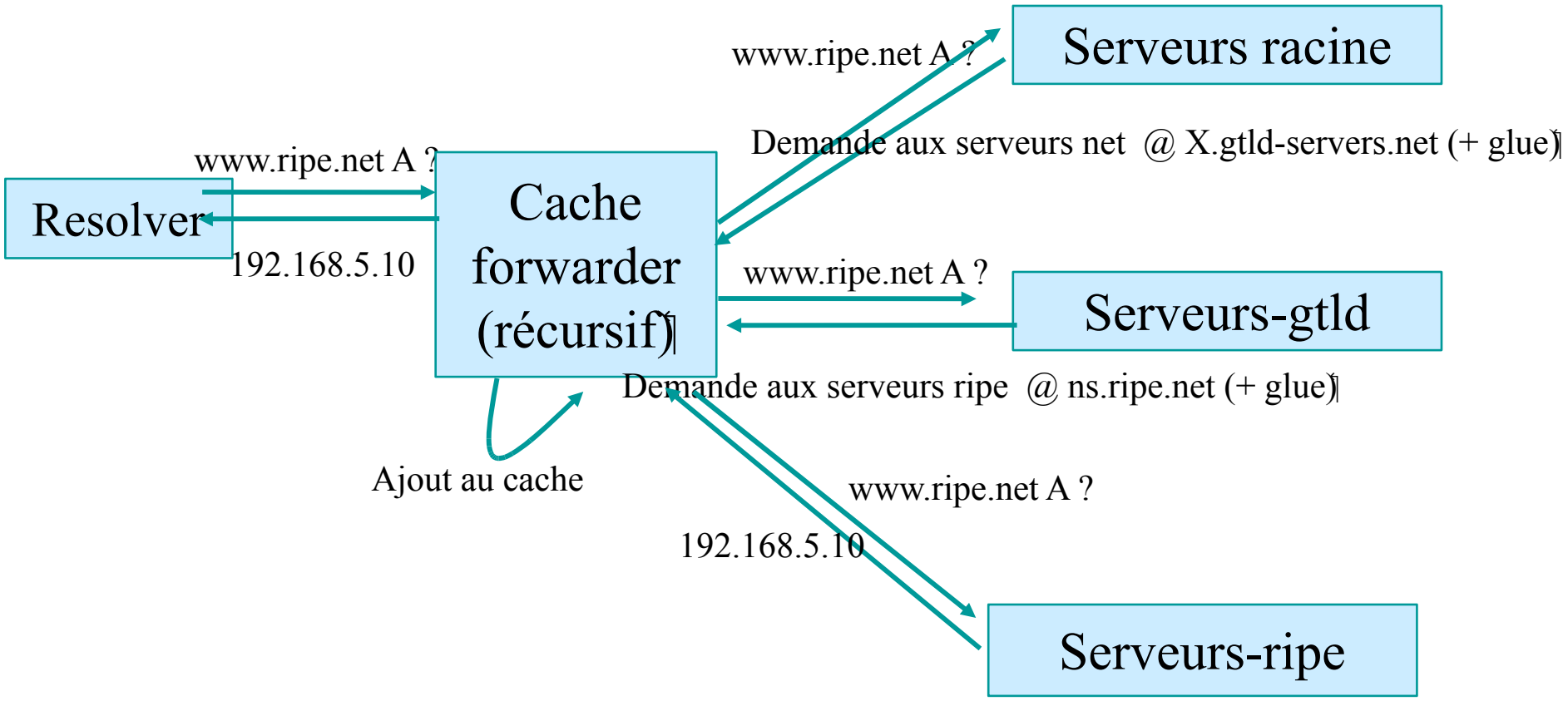


DNS
Mouvement des données

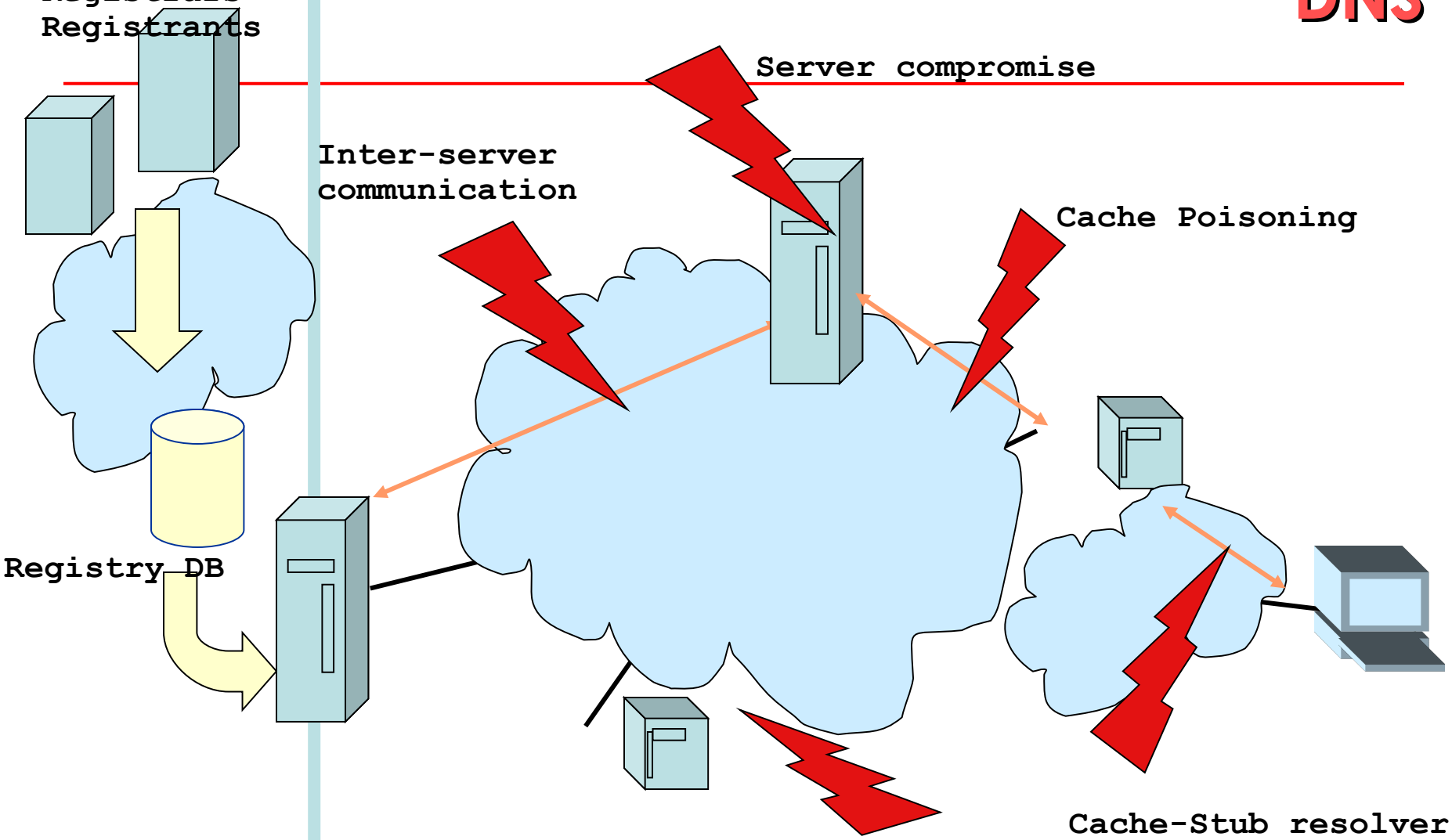


Résolution DNS

Question: www.ripe.net A



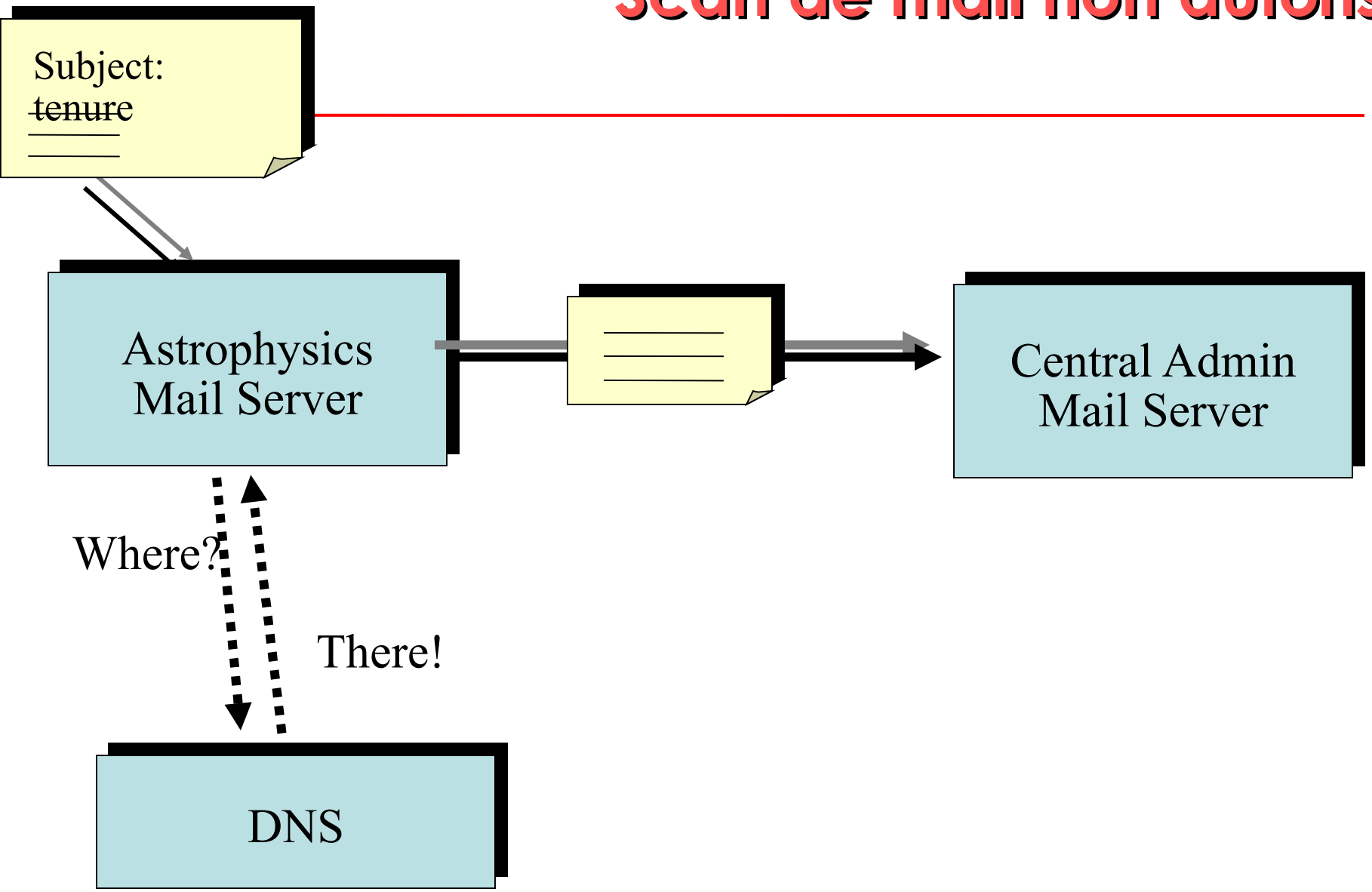
Points de vulnérabilité DNS



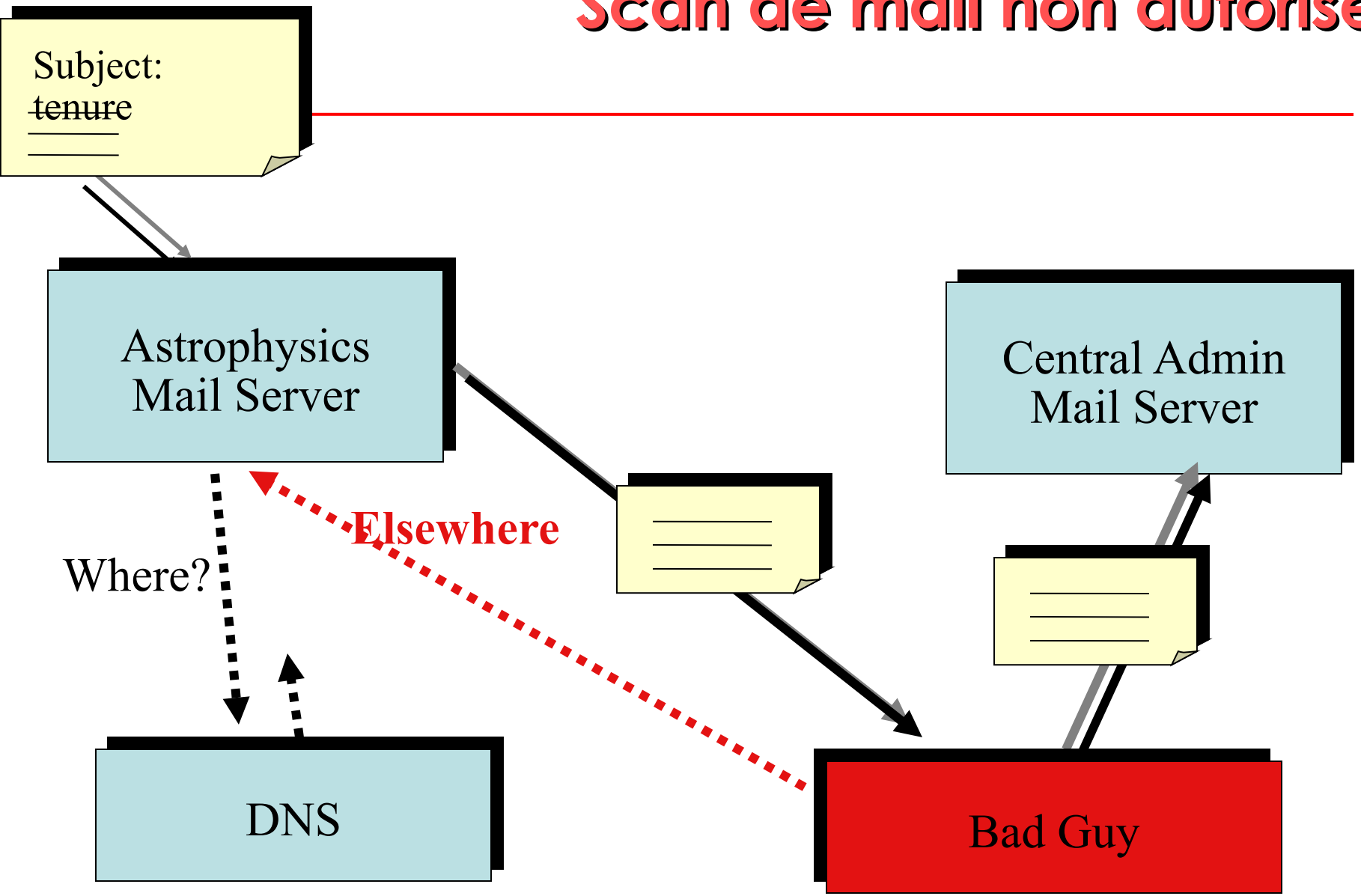
Provisioning

DNS Protocol

Exemple:
Scan de mail non autorisé



Exemple:
Scan de mail non autorisé



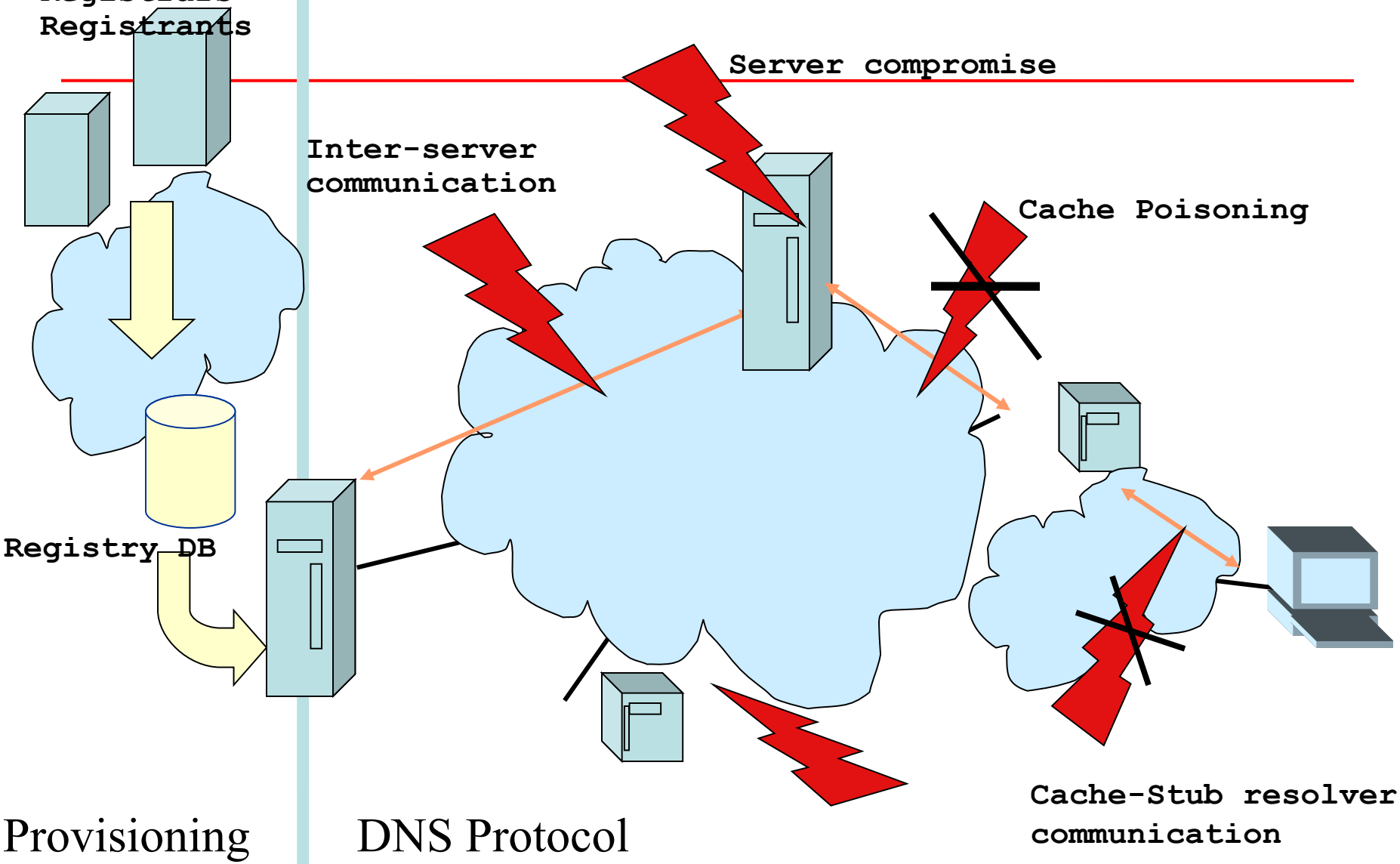
Où intervient DNSSEC?

- DNSSEC sécurise le mappage des noms en adresses IP, etc...
  - La sécurité au niveau transport et applicatif est du ressort d'autres couches.

Propriétés de DNSSEC

- DNSSEC fournit l'authentification de message et la vérification d'intégrité à travers des signatures cryptographiques
  - Source DNS Authentique
  - Pas de modifications entre signature et validation
- Il ne fournit pas d'autorisation
- Il ne prévoit pas la confidentialité

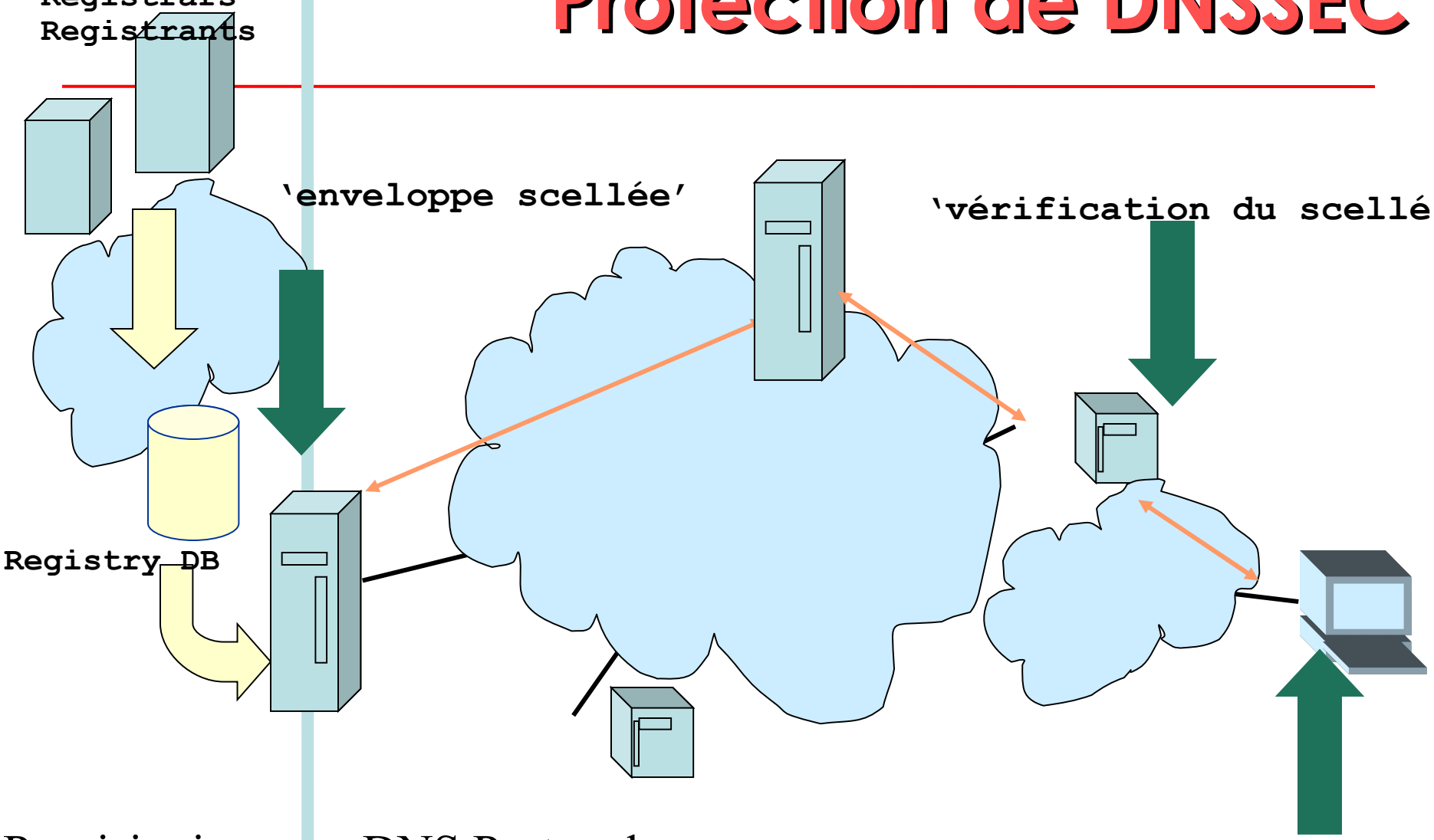
Protection de DNSSEC



Provisioning

DNS Protocol

Protection de DNSSEC



Bienfaits secondaires du DNSSEC

- DNSSEC Fournit un chemin de confiance indépendante
  - La personne qui administre “https” est certainement différente de la personne qui fait “DNSSEC”
  - Les chaînes de confiance sont probablement différentes

Autres bienfaits ?

- Avec une confiance raisonnable, on peut faire des échanges de clés opportunistes
  - SSHFP et IPSECKEY RRs
- Avec DNSSEC, le DNS peut être utilisé pour des négociations de pré-requis de sécurité.
  - “Tu ne peux accéder a ce service qu'a travers un canal sécurisé”

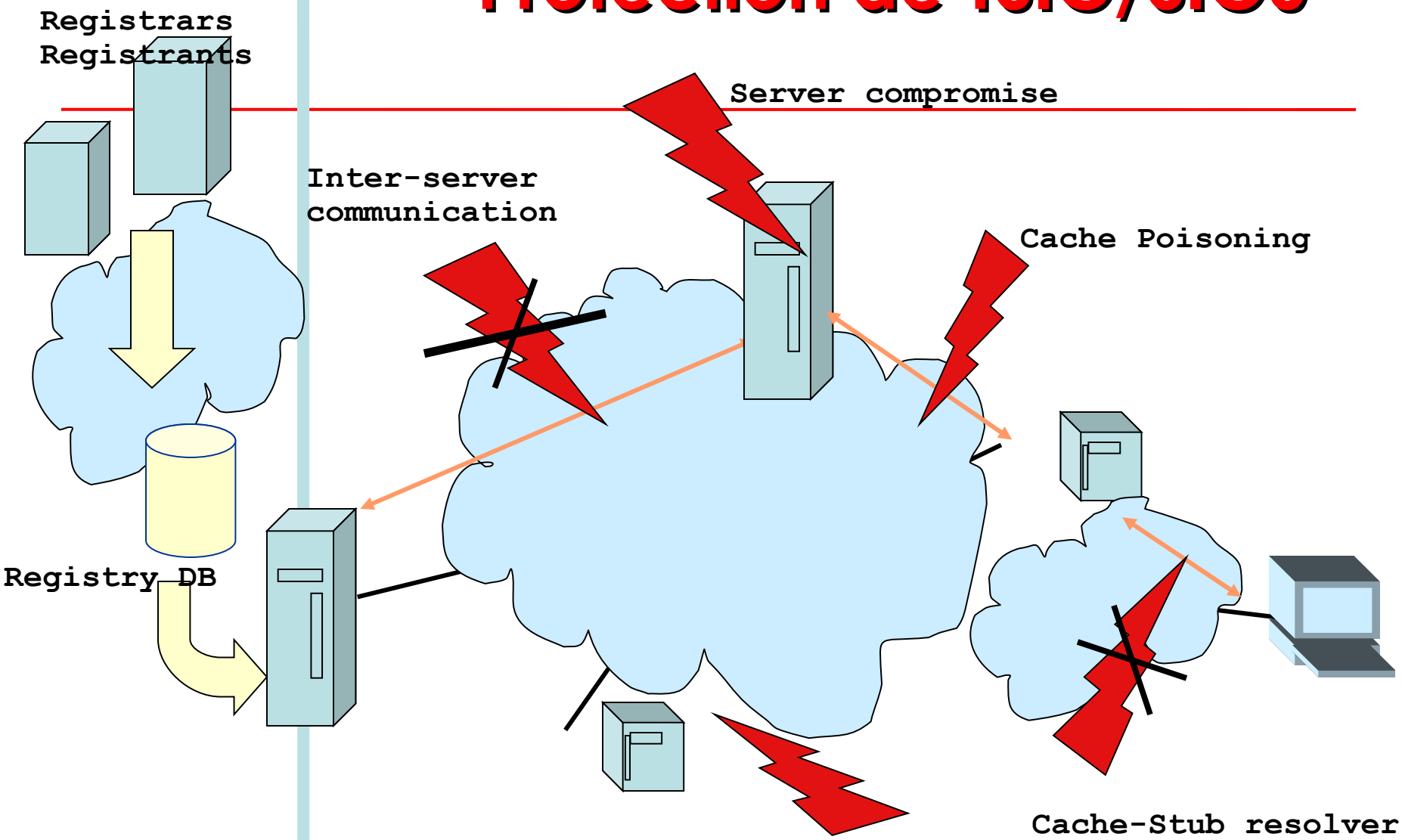
Autre mécanismes de sécurité DNS

Nous avons parlé de la protection des données

- La technologie de l'enveloppe scellée

- Il y a aussi la composante de sécurité du transport
  - Utile pour les communications bilatérales entre machines
  - TSIG ou SIG0

Protection de TSIG/SIG0



Provisioning

DNS Protocol

DNSSEC en une page

- L'authenticité et l'intégrité de données par la signature des ensembles de «ressource Record » avec la clé privée
- La clé publique est utilisée pour vérifier les RRSIGs
- L'enfant signe sa zone avec sa clé privée
  - L'authenticité de cette clé est déterminée par la signature de contrôle du parent (DS)
- Cas idéal: une clé publique distribuée

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

- Utilise deux clés : une privée et une publique
- Bref:
  - Si tu connais la clé publique, 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 (ex. factorisation)
- Algorithmes : DSA, RSA, elliptic curve, etc..
- Les clés publiques ont besoin d'être distribuées.
- Les clés privées ont besoin d'être gardées secrètes
  - Pas évident
- La cryptographie à clé publique est 'lente'

Nouveaux “ER” pour 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 consistance 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**

혼 www.ripe.net IN 7200 A 192.168.10.3

- Tout les ERs d’un “label” donné, “class”, “type” forment un “jeu” de ER:

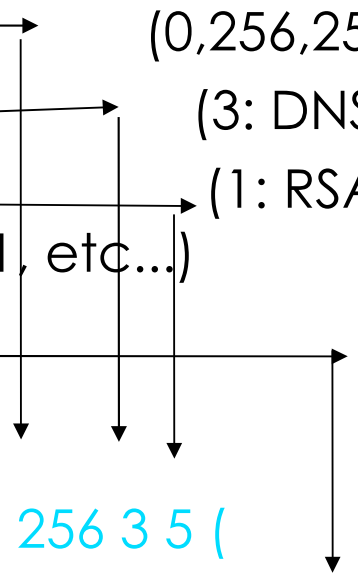
  www.ripe.net IN 7200 A 192.168.10.3

  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, etc...)
- Clé publique à N*32 bits



Exemples:

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

RSA/SHA-256 est recommandé comme remplacant de RSA/SHA1

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
- Signature

www.ripe.net. 3600 IN RR**SIG** A 1 3 3600 20010504144523 20010404144523 3112 ripe.net. (VJ+8ijXvbrTLeoAiEk/qMrdudRnYZM1VlqhNvhYuAcYKe2X/jqYfMfjfSUrmhPo+0/GOZjW66DJubZPmNSYXw==)

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):

```
ripe.net.          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 de la zone enfant en utilisant le DS
- Est un pointeur vers la 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
- XX octets de digest

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 (
                   239af98b923c023371b521g23b92da1
2f42162b1a9
                                      )
```

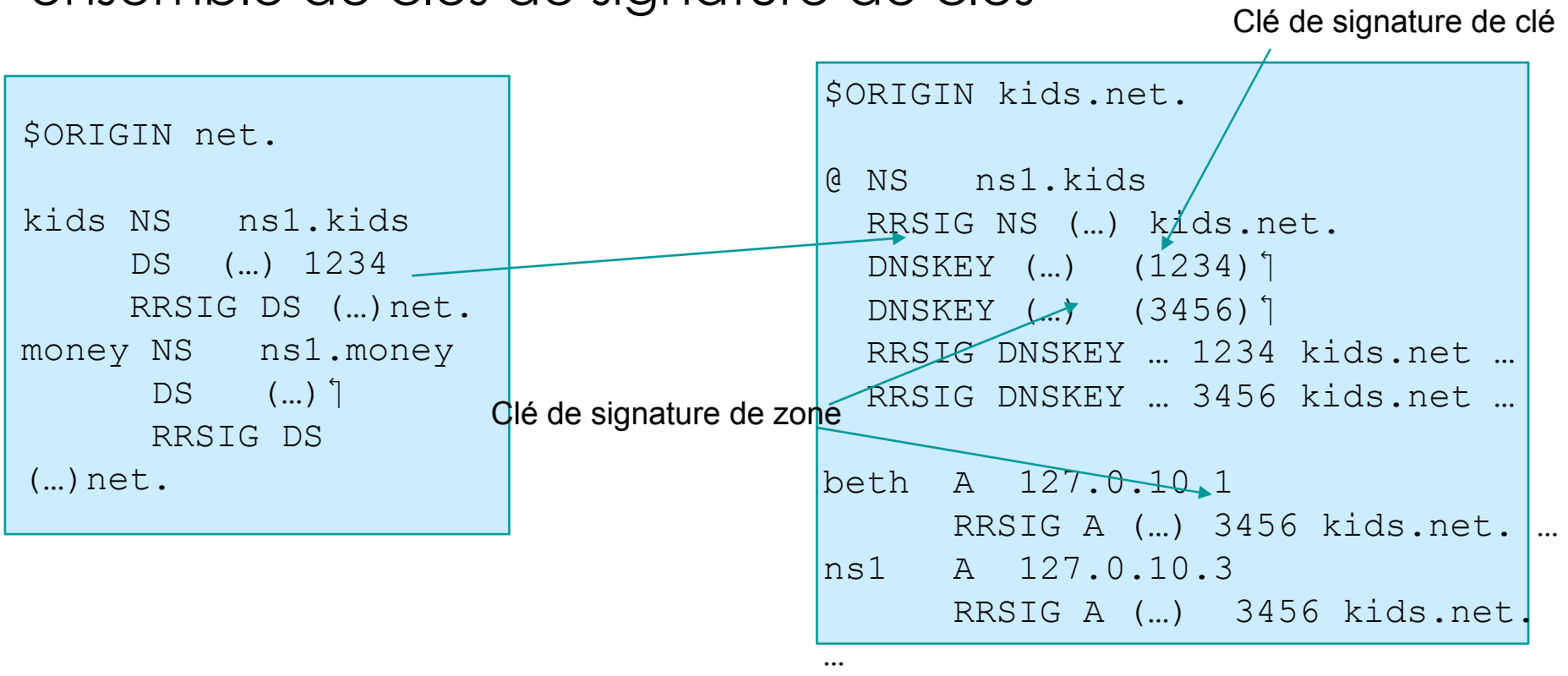
Signature de zone

- La signature accomplit les taches suivantes
  - Trier la zone
  - Insérer les enregistrement NSEC
  - Insérer RRSIG contenant une signature pour chaque “jeu” d’enregistrement de ressource.

La signature est faite avec la clé privée

Délégation de zone signée

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



KSK/ZSK

- Deux différentes clés sont utilisées
- DS pointe vers la clé de signature de clé(KSK)
- Le KSK signe les clés
- 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”

KSK/ZSK

- NIST 800-81r1 suggère
  - RSA 1024 bits pour ZSK
  - RSA 2048 bits pour KSK
  - RSA/SHA-256 dès que possible
  - Utiliser Une bonne source de nombre aléatoire
    - RFC4086
    - NIST SP 800-90

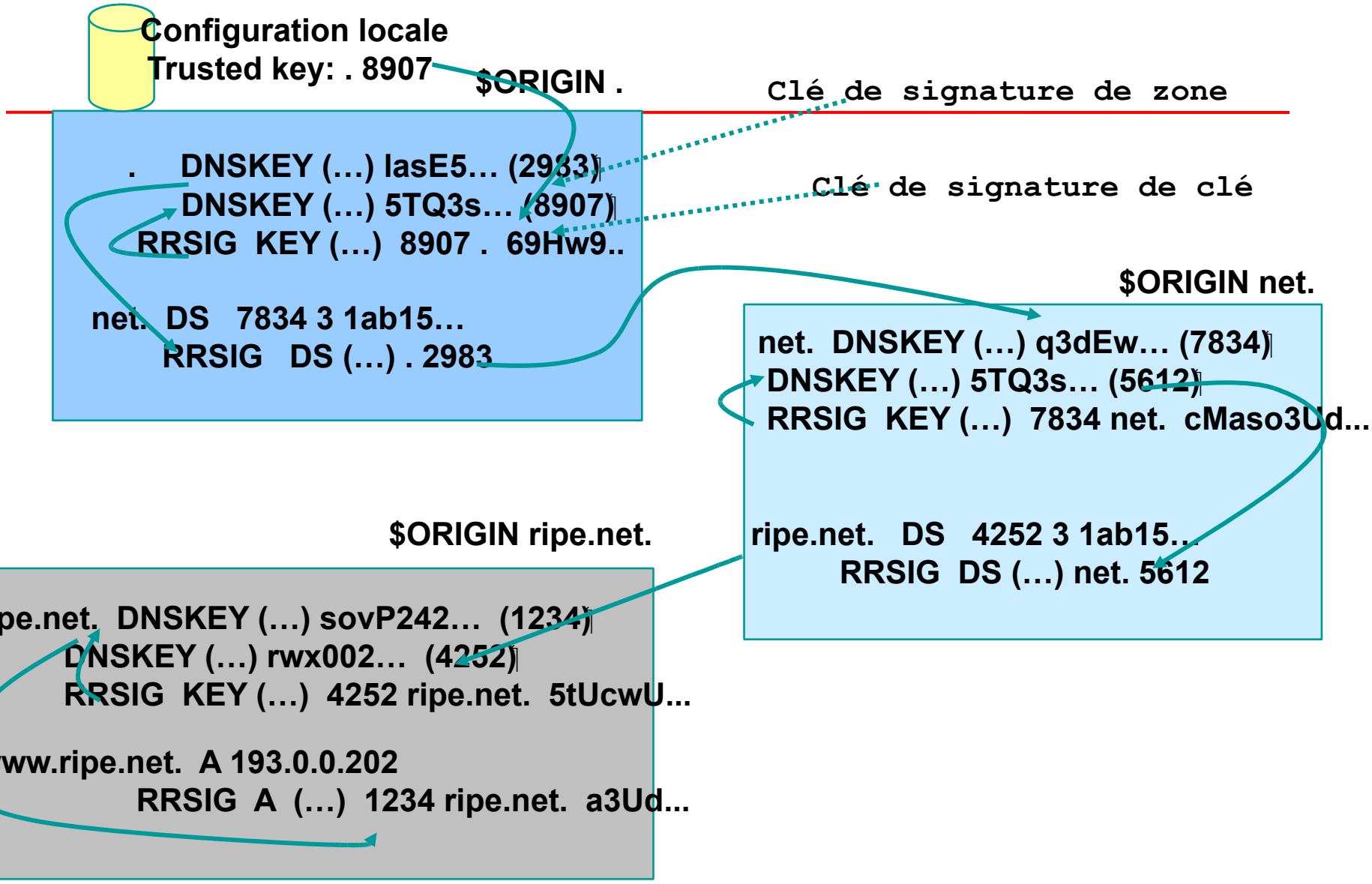
Table 9-1. Digital Signature Algorithms, Min. Key Sizes, and Crypto Periods

Key Type	Digital Signature Algorithm Suite	Key Size	Crypto Period (Rollover Period)
Key-Signing Key (KSK)	RSA-SHA1 (RSA-SHA-256) until 2015	2048 bits	12-24 months (1-2 years)
Zone-Signing Key (ZSK)	RSA-SHA1 (RSA-SHA-256) until 2015	1024 bits	1-3 months (30-90 days)

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 digne de confiance 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 KSK peut être valide si elle est échangée hors bande (Trusted key)

Chaîne de confiance



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

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 sauf pour des données qu'il contrôle et s'il est configuré pour..
- AD = Authenticated data(donnée authentique)

Bit CD

- Un bit d'état dans la section « header » des paquets DNS
  - Non utilisé avant DNSSEC(devrait être à zéro)
- CD = Checking Disable (validation désactivée)
  - 1= validation désactivée
    - Le “resolver” accepte des réponses non vérifiées
  - 0= validation 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)
  - 1= le "resolver" veut les enregistrements DNSSEC
  - 0= le "resolver" ne veut pas les enregistrements DNSSEC

Utilisation du DNS pour distribuer les clés

- Les îles sécurisées rendent problématique la distribution de clés
- Distribution de clés par le biais du DNS:
  - Utiliser une clé de confiance pour établir l'authenticité des autres clés
  - Construire des chaînes de confiance de la racine vers le bas
  - Les parents ont besoin de signer les clés de leurs enfants
- Seul la clé racine est nécessaire dans un monde idéal
  - Les parents délèguent toujours la sécurité à l'enfant

... Mais il n'est pas intéressant de signer votre zone si le parent ne signe pas ou n'est pas signé ...

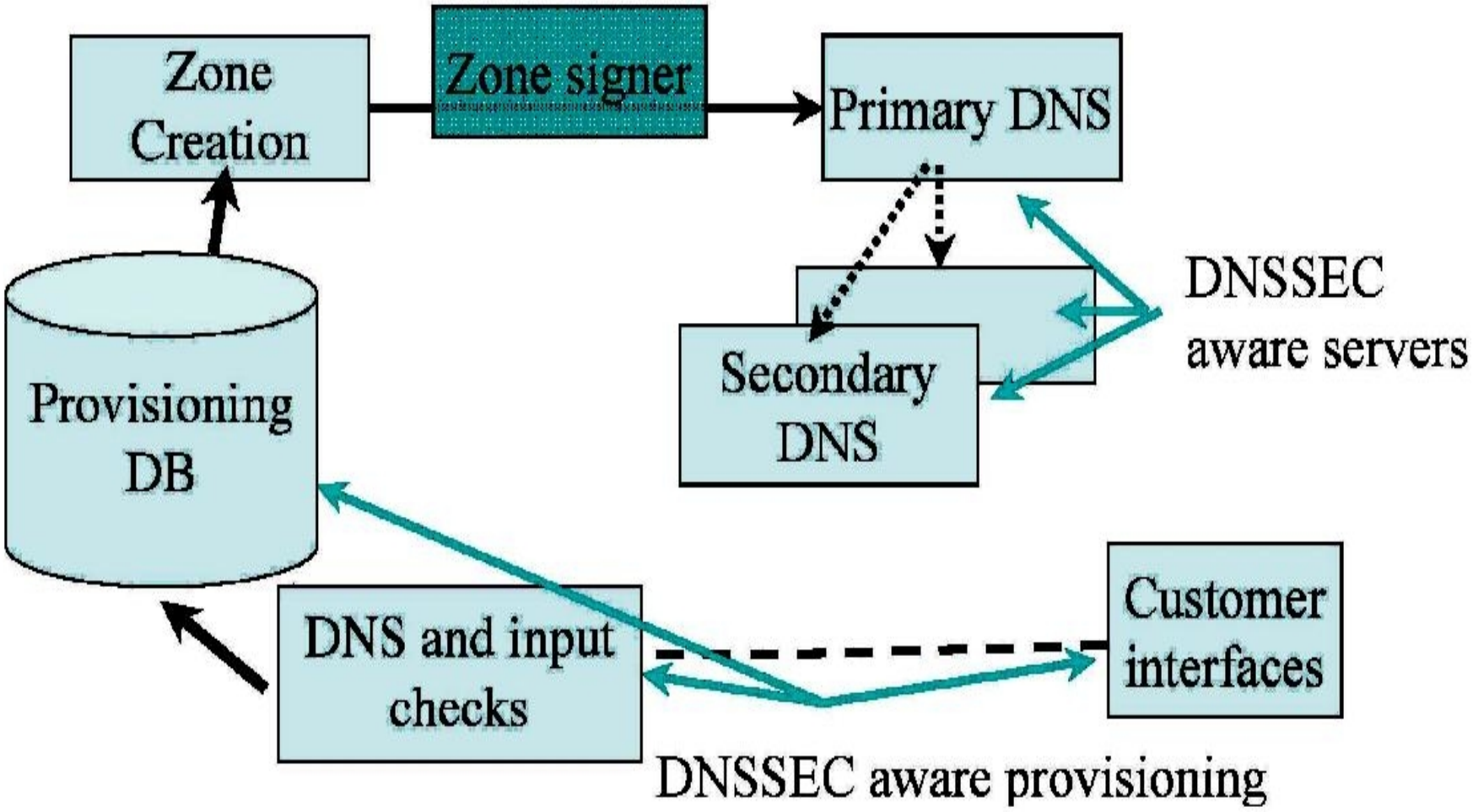
Utilisation du DNS pour distribuer les clés

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

Tâches de déploiement de DNSSEC

- Politiques et outils de gestion des clés
  - Utilisation et protection de la clé privée
  - Distribution de la clé publique
- Signature et Intégration de zone dans la chaîne d'approvisionnement
- Infrastructure de serveurs DNS
- Délégation sécurisée des modifications du registre
  - Interfaçage avec les clients

Modification de l'Architecture DNS



Quelques Hics avec DNSSEC

- Ne protége pas contre les attaques de déni de service; mais en augmente les risques
  - **Charge de travail cryptographique**
  - **Longeur des message DNS**
  - **RFC5358**
- 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
- Comment se fera la distribution et le renouvellement du Trust Anchor(KSK de la racine) ?
  - **RFC5011 ??**

Quelques Hics avec DNSSEC

- DNSSEC introduit un mécanisme qui permet de lister tous les noms d'une zone en suivant la chaîne NSEC
  - **NSEC3 si le "zonewalk" est un problème pour vous**
- Certains firewalls/middle box ne supportent pas des paquets DNS > 512 Octets(edns0)
  - **Beaucoup sont reconfigurables**
- Certains Firewalls/middle box ont des soucis avec les bits AD,CD,DO
- Certains vieux resolvers peuvent avoir des soucis avec le bit AD
  - **Faire mettre le bit AD dans les requêtes pour signaler l'état des resolvers ?**

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
  - RFC4641
  - http://tools.ietf.org/id/draft-ietf-dnsop-rfc4641bis-01.txt

Questions?