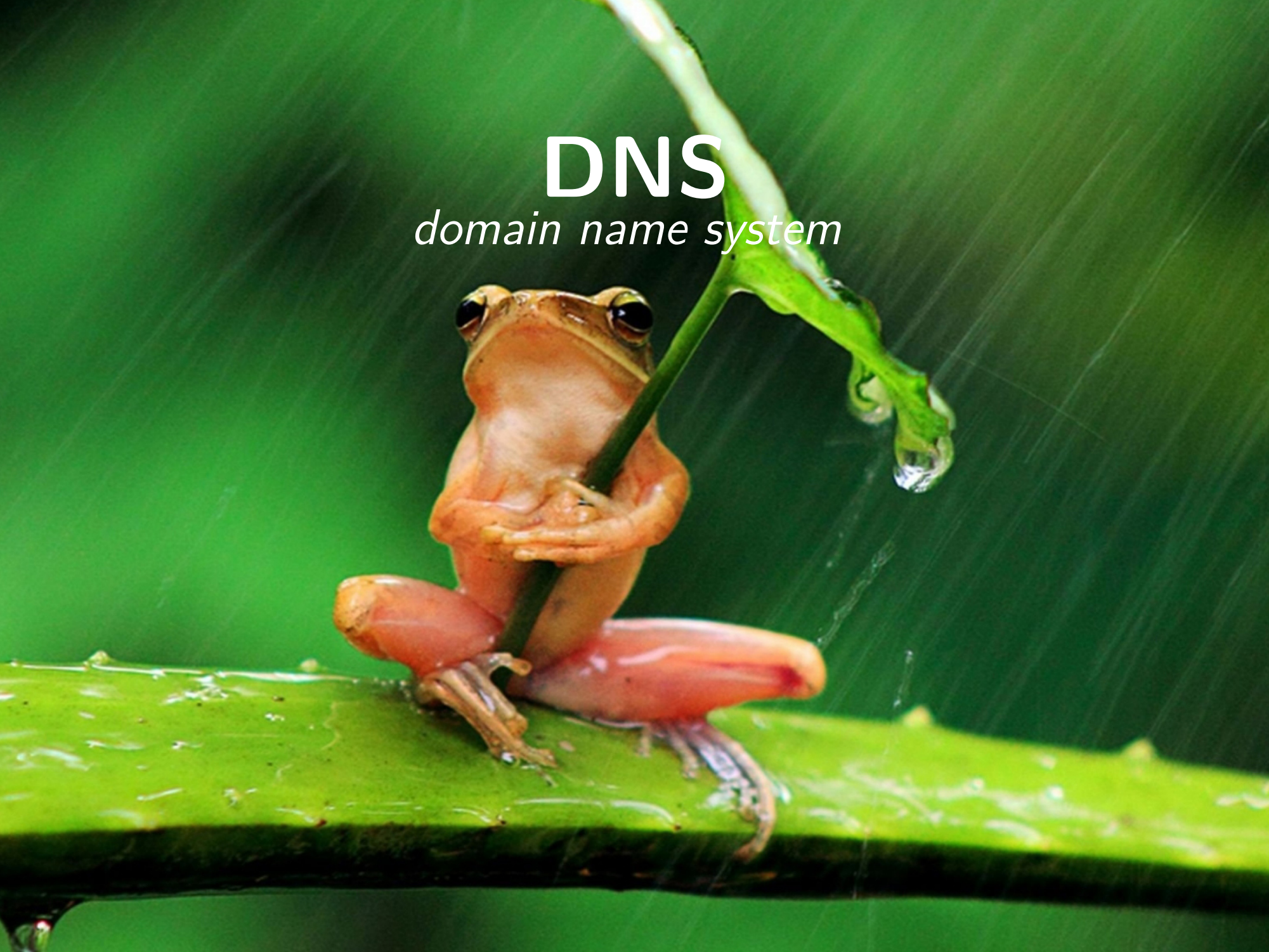
DNS - Domain Name System

Pierre Bettens

septembre 2023
v0.2 ~ October 6, 2023


DNS
domain name system

Les adresses IP n'étant pas très conviviales, nous retenons les noms de machines...

... un server de noms permet la **correspondance** nom / IP.

Résolution

La résolution de noms peut se faire de différentes manières (cfr. `/etc/nsswitch.conf`)

- Table d'hôtes : `/etc/hosts`
- Multicast DNS `mdns`
- Serveur DNS

Quels noms ?

Noms locaux

`localhost.localdomain` - `l001p01.intranet.example.org` - ...

Noms internet

`pica.esigoto.info` - `monserver.example.org` - ...


Explosion des noms de domaines de premier niveau
genèse, 2000, 2014

Noms de domaine

- Genèse

  `com`, `edu`, `gov`, `mil`, `net`, `int`, `org` et *géographiques*

- 2000

  `aero`, `biz`, `coop`, `museum`, `pro`, `info`, `name`

- 2014

  https://www.iana.org/domains/root/db

ba baby baidu banamex bananarepublic band bank bar barcelona barclaycard barclays barefoot bargains baseball basketball bauhaus bayern bb bbc bbt bbva bcg bcn bd be beats beauty beer bentley berlin best bestbuy bet bf bg bh bharti bi bible bid bike bing bingo bio biz bj black blackfriday blockbuster blog bloomberg blue bm bms bmw bn bnpparibas bo boats boehringer bofa bom bond boo book booking bosch bostik boston bot boutique box br bradesco bridgestone broadway broker brother brussels bs bt build builders business buy buzz bv bw by bz bzh

DNS - Fonctionnement

DNS est *acentralisé* [1]

- permet la gestion du nombre
- dissémine / répartit l'information
- résilient

Important

Sans DNS, Internet *est cassé*

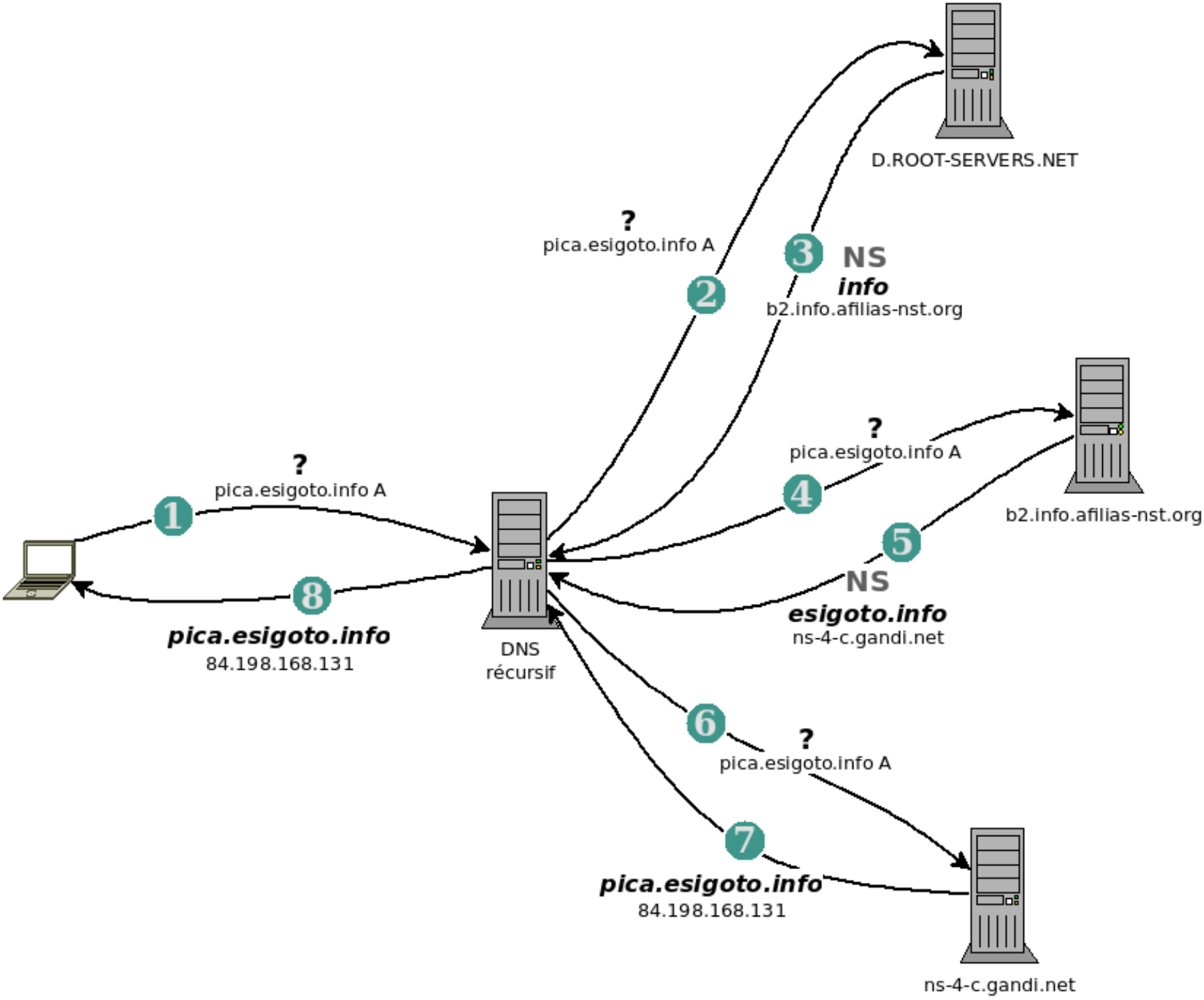
[1] *a* privatif. Sans centre. Comme Internet

DNS - Fonctionnement

Fonctionnement *top / down* avec *cache*...

- Si le serveur a la réponse en cache ou d'autorité, il répond;
- sinon, il *fait une requête récursive* auprès des différents serveurs ayant autorité.

Le propriétaire (en fait locataire) de la zone (par ex. `example.org`) maintient son fichier de zone (voir plus loin) et « son serveur » DNS a autorité pour cette zone.


D.ROOT-SERVERS.NET
?
pica.esigoto.info A
2
3
NS
info
b2.info.afilias-nst.org
?
pica.esigoto.info A
1
4
b2.info.afilias-nst.org
5
NS
esigoto.info
ns-4-c.gandi.net
8
pica.esigoto.info
84.198.168.131
DNS
récursif
6
?
pica.esigoto.info A
7
pica.esigoto.info
84.198.168.131
ns-4-c.gandi.net

DNS - Fonctionnement

Quelques tests

```
dig esigoto.info
dig esigoto.info +trace

dig . NS @a.root-servers.net
```

Q ? Faire de même avec l'option `+nordflag` (*no recursion desired*).
Q ? Que signifient les *flags* retournés par `dig` ?

Pour localiser une IP,
`curl https://ipapi.co/<IP>/yaml -s`

DNS Logiciels

Le client (*stub resolver*) est le programme qui va faire la requête auprès d'un serveur complet :

- configuré dans `/etc/resolv.conf`
- navigateur internet, `dig`...

Le résolveur complet (*full resolver*) est le programme qui peut faire la requête récursive :

- `bind`
- `unbound`
- ...

Le serveur ayant autorité (*authoritative server*)

- `bind`
- ...


fichiers de zone

DNS - Fichiers de zone

Une zone est composée de différents types de champs :

SOA, NS, A, AAAA, PTR, MX, CNAME, TXT...

DNS - Fichiers de zone

Exemple de la zone locale

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@   IN  SOA localhost. root.localhost. (
                  2     ; Serial
             604800     ; Refresh
              86400     ; Retry
            2419200     ; Expire
             604800 )   ; Negative Cache TTL
;
@   IN  NS  localhost.
@   IN  A   127.0.0.1
@   IN  AAAA    ::1
```

DNS - Fichiers de zone

Enregistrement `SOA`

- serveur maitre principal de la zone
- adresse email du responsable de la zone (avec `@` remplacé par `.`)
- numéro de série. Convention : `YYYYMMDDVV`
- *Refresh* temps après lequel un serveur secondaire vérifie si une mise à jour est nécessaire.
- *Retry* temps après lequel, un serveur secondaire réessaie s'il n'avait pas eu de réponse. $Retry < Refresh$
- *Expire* temps après lequel, il abandonne. $Expire > Refresh + Retry$
- *TTL* durée de validité d'une réponse négative (cfr. RFC2308)

Recommandation pour les petits zones stables **24h 2h 6w 3h**

DNS - Fichiers de zone

Exemple d'une zone pour example.org

```
;
; BIND data file for example.org zone
;
$TTL    24h
@   IN  SOA example.org. root.example.org. (
    2017010101 24h 2h 42d 3h);
@       IN  NS  ns
@       IN  MX  5 mail
@       IN  MX  10 mail.isp.net.
ns      IN  A   93.94.106.205
ns      IN  AAAA 2a00:1140:2:2::8
serveur IN  A 46.105.92.142
serveur IN  AAAA 2001:41d0:401:3100::4ffe
mail    IN  CNAME serveur
```

dns menteur

DNS - RPZ response policy zone

DNS menteur ou *response policy zone* (**RPZ**).

Depuis la version `9.8.0` de `bind9`, un DNS peut mentir.

Dans la configuration du serveur DNS, précisez dans les options, quelle zone correspond à *response_policy* et définir la zone ou la récupérer de *quelque part* (entreprise, état...)

```
options {
    // ...
    response-policy { zone "liar.local";};
};
```

Lien bortzmeyer.org

Lien blog.namok.be

DNSSEC

DNSSEC

DNSSEC est une extension de sécurité à DNS.

Il ajoute des signatures crypotgraphiques pour les enregistrements. Les données d'une zone sont signées afin de pouvoir être vérifiées.

DNSSEC ajoute à DNS :

- l'**authentification** de l'origine des données;

  Les données proviennent bien du serveur supposé être la source.

- l'**intégrité** des données;

  Les données n'ont pas été altérées en chemin. Elles ont été signées par le propriétaire de la zone et je peux le vérifier.

- un **chainage de confiance** (voir plus loin)

Clé de signature de zone ZSK

Chaque **zone** DNS a une paire de clés publique-privée.

Cette clé (ZSK) est utilisée pour signer les données de la zone. La partie publique de la clé se trouve dans l'enregistrement DNSKEY

```
dig <name> DNSKEY +multi
```

```
;; ANSWER SECTION:
example.org.    3564 IN DNSKEY 256 3 13 (
                    hN+W90ybHRZT2qZM[cut]ZoOq8WHONiOeVQtn
                    LJPszWFr1UYUzuSV[cut]EaZf702W2GzdmcQ==
                ) ; ZSK; alg = ECDSAP256SHA256 ; key id = 64700
```

DNSSEC

DNSSEC ajoute les champs suivants :

`DNSKEY`, `RRSIG`, `DS`, `NSEC`, `NSEC3`, `CDNSKEY`, `CDS`

DNSSEC

- `DNSKEY` la partie publique de la clé
- `RRSIG` contient le signature cryptographique du `RRset` correspondant
- `DS` le *hash* de la `DNSKEY`
- `NSEC` et `NSEC3` pour le déni d'existence explicite d'un enregistrement
- `CDNSKEY` et `CDS` pour une zone enfant demandant des mises à jour dans la zone parent

(voir la suite)

RRsets

Rassemble des enregistrements de même type pour un même *label* (Par ex. `host.example.org`). C'est cet ensemble qui sera signé.

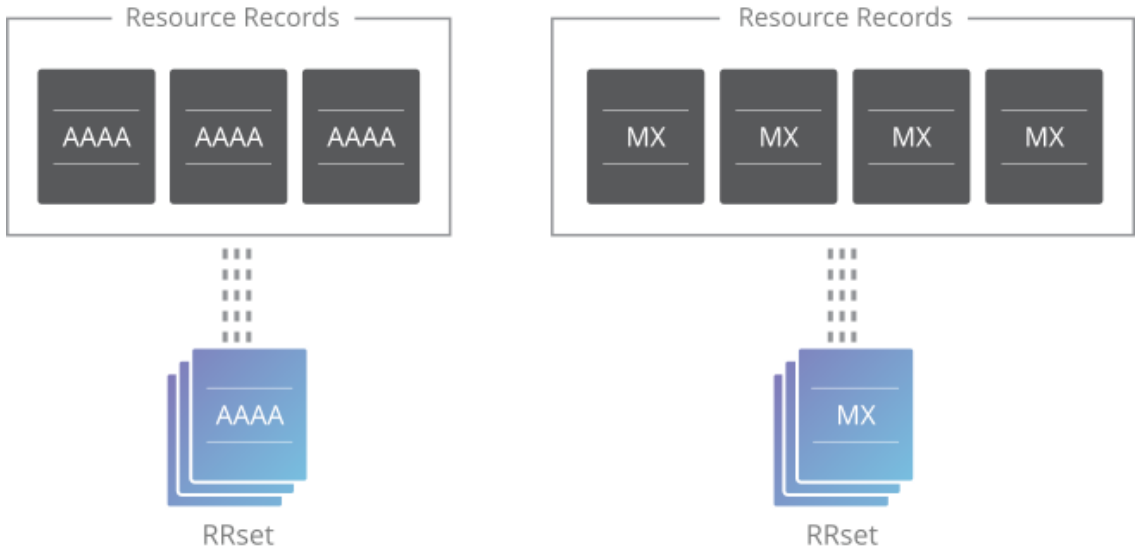


Figure 1: Source Cloudflare

DNSSEC

```
dig example.org  +dnssec
```

```
example.org.    4214 IN A 93.184.216.34
example.org.    4214 IN RRSIG A 13 2 86400 (
                    20231013015700 20230922122122 64700 example.or
                    6gn68jzj2mdSAfY+4IzcHvlg5geEvasp6+xWSJX7v+MC
                    GFTMmQpp42CoXePyKkxJYi0HHlzhrlHazZ3D0BmQvQ== )
```

- A: le type d'enregistrement
- 13 : l'algorithme utilisé
- 2 : le nombre de labels du RRSet
- 86400 : le TTL originel
- 20231013015700 : la date d'expiration
- 20230922122122 :
- 64700 : *keytag* (identifiant non-unique de la clé)
- example.org : nom du signataire
- ... : la signature

Ensemble, *RRset*, *RRSIG* et la *DNSKEY* peuvent valider la réponse.

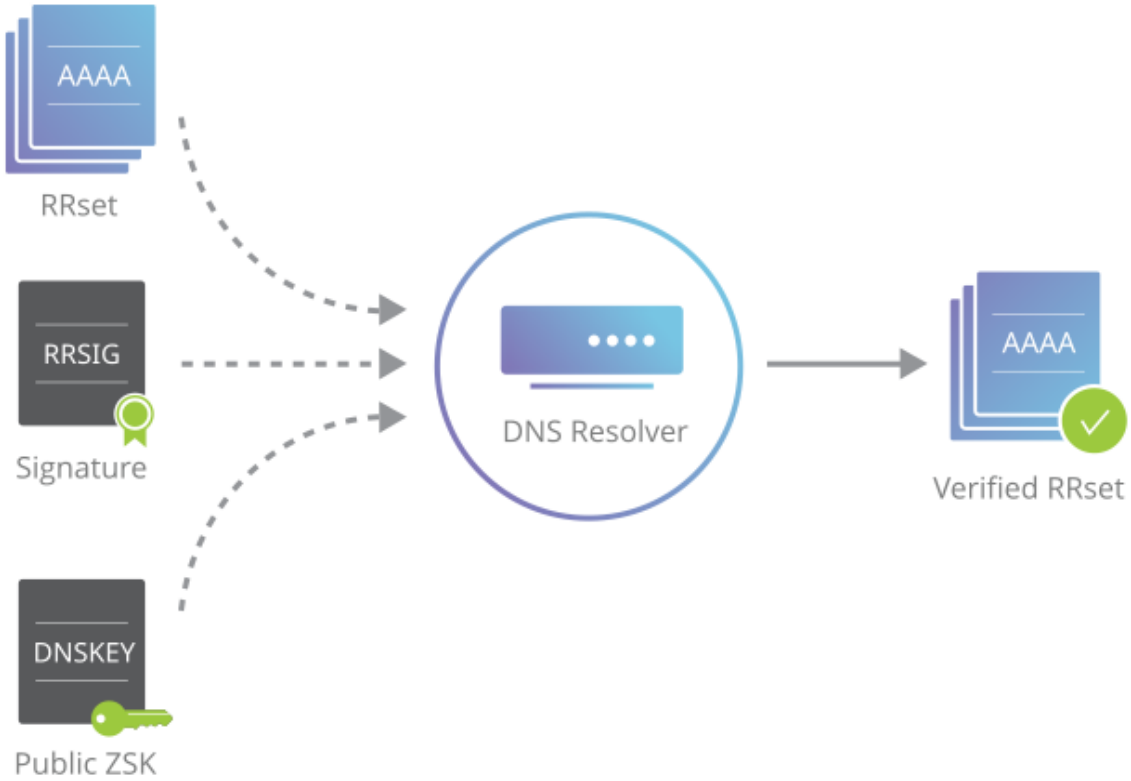


Figure 2: Source Cloudflare

Clé de signature de clé KSK

La clé ZSK est utilisée pour signer les *RRsets*.

De même la clé KSK (*key signing key*) est utilisée pour signer la ZSK.

Chaine de confiance

Comment être sûr de l'authenticité de la clé publique (KSK) ?

En *hashant* cette clé et en fournissant le *hash* à la **zone parent**. Ce *hash* se trouve dans l'enregistrement `DS`.

De parent en parent, ceci établit une chaine de confiance.

`.` signe `.org` qui signe `example.org`…

DNSSEC

```
dig ds example.org [+dnssec] +multi
```

```
example.org.    732 IN DS 22273 13 2 (
                    71405420F[cut]D58737
                    60E24A3B4DC61A964FEE )
```

Les enregistrements NSEC et NSEC3 permettent de « signer » les réponses vides précisant qu'une zone n'existe pas.

NSEC est réputé sensible à *zone walking attack*. NSEC3 moins.

DNSSEC

```
dig A +dnssec a.dnstests.ovh
dig A +dnssec sub.dnstests.ovh
```

```
dnstests.ovh.   12  IN  NSEC sub.dnstests.ovh.
        A NS SOA RRSIG NSEC DNSKEY

sub.dnstests.ovh.   3600    IN      A       1.2.3.4
sub.dnstests.ovh.   3600    IN      RRSIG
        A 8 3 3600 20231101075445
        20231002075445 44275 dnstests.ovh. o+H7SO0/y[cut]PgT gWo=
```

DNSSEC

```
dig A +dnssec public.example.org
```

```
22cse7p1cuuea0185da5kpjrmajk5gpr.example.org. 3535 IN
        NSEC3 1 0 5
        B014[cut]BU A NS SOA MX TXT AAAA RRSIG DNSKEY NSEC3PARAM
```

bind9

bind

Mise en place de bind9

```
apt install bind9
```

Fichiers de configuration :

```
/etc/bind/
├── bind.keys
├── db.0
├── db.127
├── db.255
├── db.empty
├── db.l504.org
├── db.local
├── db.root
├── named.conf
├── named.conf.default-zones
├── named.conf.dpkg-dist
├── named.conf.local
├── named.conf.options
├── named.conf.options.dpkg-dist
├── rndc.key
└── zones.rfc1918
```

unbound

unbound

Mise en place de unbound

```
apt install unbound
```

Fichiers de configuration :

```
/etc/unbound/
├── unbound.conf
├── unbound.conf.d
    ├── qname-minimisation.conf
    └── root-auto-trust-anchor-file.conf
├── unbound_control.key
├── unbound_control.pem
├── unbound_server.key
└── unbound_server.pem
```