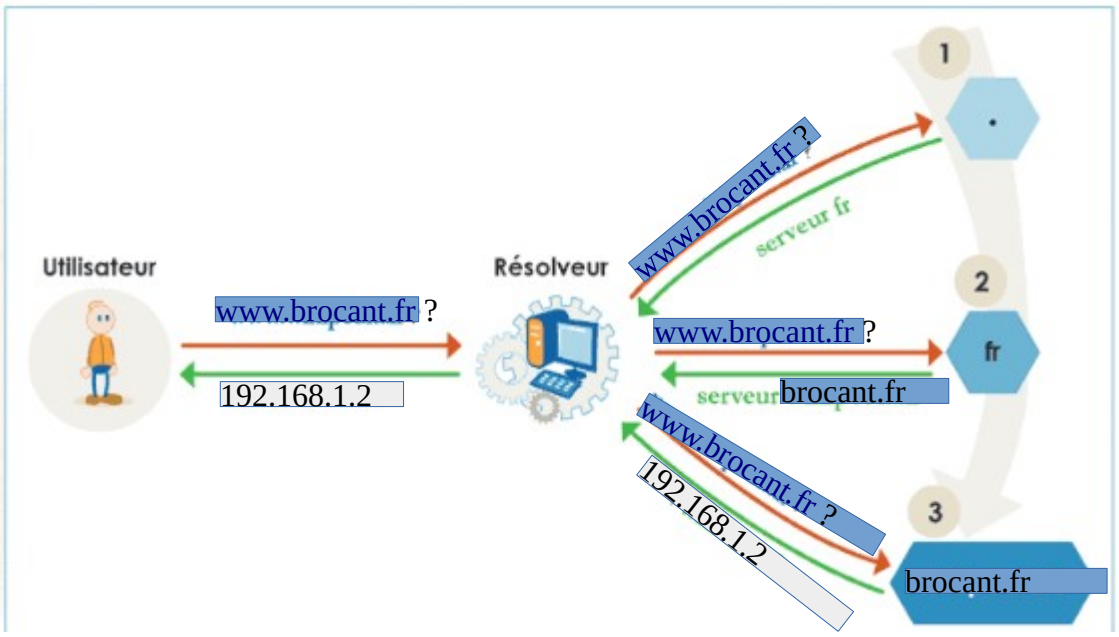
Documentation Technique : Mise en place de dnssec pour sécuriser le DNS du domaine (brocant.fr)



DNSSEC utilise un mécanisme reposant sur une paire de clés ayant des rôles complémentaires. La première clé, privée, crée une signature par chiffrement; alors que la seconde clé, publique, vérifie les signatures par déchiffrement:

Mise en place de DNSSEC sur le serveur DNS

Nom des zones :

- **Brocant.fr** est notre nom de domaine
- **1.168.192-in.addr.arpa** est notre zone de reverse

Fichier de zone :

- **db.brocant.fr** est notre fichier de configuration qui se trouve dans /etc/bind.
- **db.192.168.1.rev** est notre fichier de configuration de la zone reverse qui se trouve dans /etc/bind.

Génération des clés ZSK et KSK pour notre nom de domaine brocant.fr et la zone reverse

- Pour la zone brocant.fr :

On crée une Zone Signing Key (ZSK) avec une clé de 4096 bits en RSASHA256 avec la commande suivante :
La commande doit être taper sur etc/bind/
dnssec-keygen -a RSASHA256 -b 4096 -n ZONE **brocant.fr**

On crée ensuite une **Key Signing Key (KSK)**, toujours avec une clé de 4096 bits en RSASHA256 :
dnssec-keygen -f KSK -a RSASHA256 -b 4096 -n ZONE **brocant.fr**

Génération des clés ZSK et KSK pour la zone 1.168.192-in.addr.arpa

On crée aussi une **Zone Signing Key (ZSK)** avec une clé de 4096 bits en RSASHA256 avec la commande suivante :
La commande doit être taper sur /etc/bind
dnssec-keygen -a RSASHA256 -b 4096 -n ZONE **1.168.192-in.addr.arpa**

On crée ensuite une **Key Signing Key (KSK)**, toujours avec une clé de 4096 bits en RSASHA256 :
dnssec-keygen -f KSK -a RSASHA256 -b 4096 -n ZONE **1.168.192-in.addr.arpa**

Les deux commandes précédentes ont créé 8 nouveaux fichiers de clés dans notre répertoire – une paire de clés publiques/privées pour ZSK et une autre paire de clés publiques/privées pour KSK.

```
K1.168.192.in-addr.arpa.+008+16605.private
K1.168.192.in-addr.arpa.+008+38269.key
K1.168.192.in-addr.arpa.+008+38269.private
Kbrocant.fr.+008+28945.key
Kbrocant.fr.+008+28945.private
Kbrocant.fr.+008+37981.key
Kbrocant.fr.+008+37981.private
```

```
K1.168.192.in-addr.arpa.+008+16605.key
```

Ajout des clés publiques dans le fichier de zone

On ajoute ensuite les quatre clés publiques qui contiennent les enregistrements DNSKEY dans le fichier de zone « **db.brocant.fr** » pour celles de la zone brocant.fr et dans le fichier **db.192.168.1.rev** pour celles de la zone **1.168.192-in.addr.arpa**

Pour ajouter les deux clés publiques dans les fichiers de zone db.brocant.fr on effectue les commandes suivantes :
echo « $include Kbrocant.fr.+008+28945.key » ” db.brocant.fr
echo « $include Kbrocant.fr.+008+37981.key » ” db.brocant.fr

Pour ajouter les deux clés publiques dans les fichiers de zone **db.192.168.1.rev** on effectue les commandes suivantes :
echo « $include K1.168.192.in-addr.arpa.+008+16605.key » ” **db.192.168.1.rev**

echo « $include K1.168.192.in-addr.arpa.+008+38269.key » ” **db.192.168.1.rev**

Signature de la zone brocant.fr

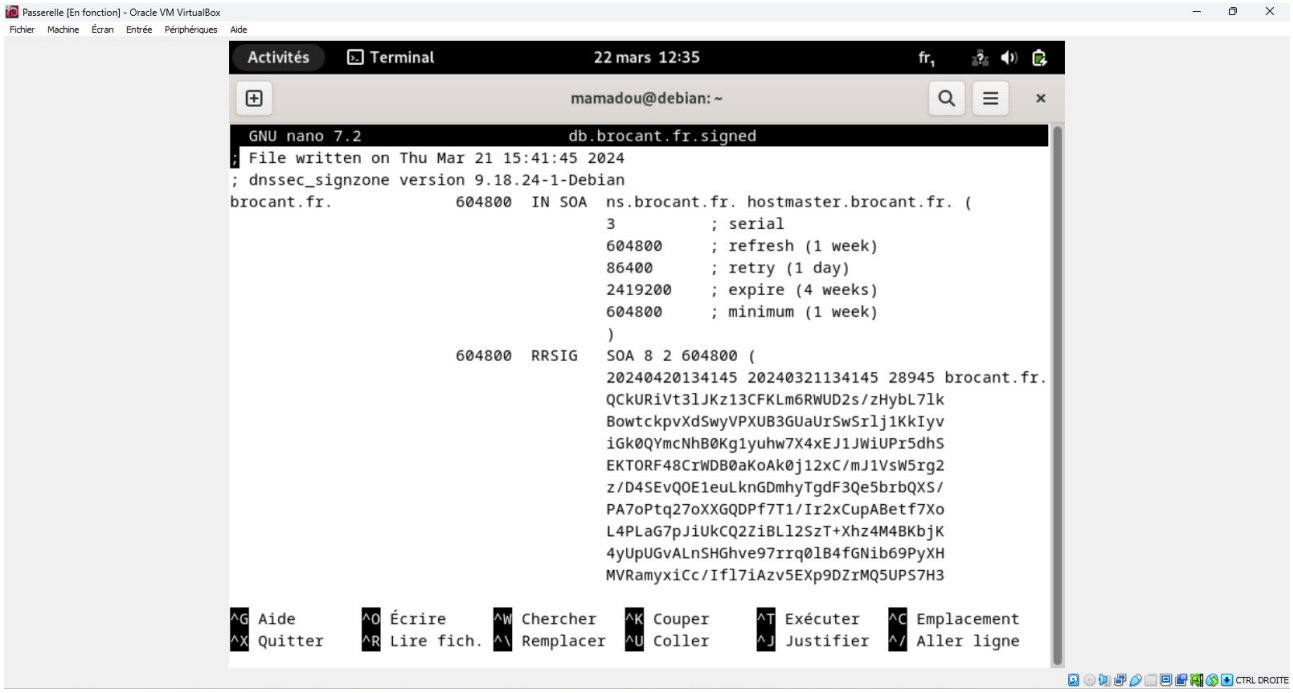
On signe maintenant notre zone « brocant.fr » avec la commande :

dnssec-signzone -A -3 $(head -c 1000 /dev/random | sha1sum | cut -b 1-16) -N INCREMENT -o brocant.fr -t db.brocant.fr

Resultat :

```
Verifying the zone using the following algorithms:
RSASHA256.
Zone fully signed:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0
revoked
 ZSKs: 1 active, 0 stand-by, 0 revoked
skyminds.net.hosts.signed
Signatures generated: 42
Signatures retained: 0
Signatures dropped: 0
Signatures successfully verified: 0
Signatures unsuccessfully verified: 0
Signing time in seconds: 0.378
Signatures per second: 110.937
Runtime in seconds: 0.442
```

Notre zone est signée avec un nouveau fichier **db.brocant.fr.signed qui** vient d’être créé



Signature de la zone 1.168.192-in.addr.arpa

On signe la zone **1.168.192-in.addr.arpa** avec la commande :

dnssec-signzone -A -3 $(head -c 1000 /dev/random | sha1sum | cut -b 1-16) -N INCREMENT -o 1.168.192-in.addr.arpa -t db.192.168.1.rev

La zone est signé avec un nouveau fichier nommé db.192.168.1.rev.signed

```
db.192.168.1.rev.signed
db.255
db.brocant.fr.signed
```

Ajout de la zone signée dans la configuration BIND

Pour ajouter la zone signée dans la configuration BIND, on commence par éditer d'abord le fichier de configuration de BIND:

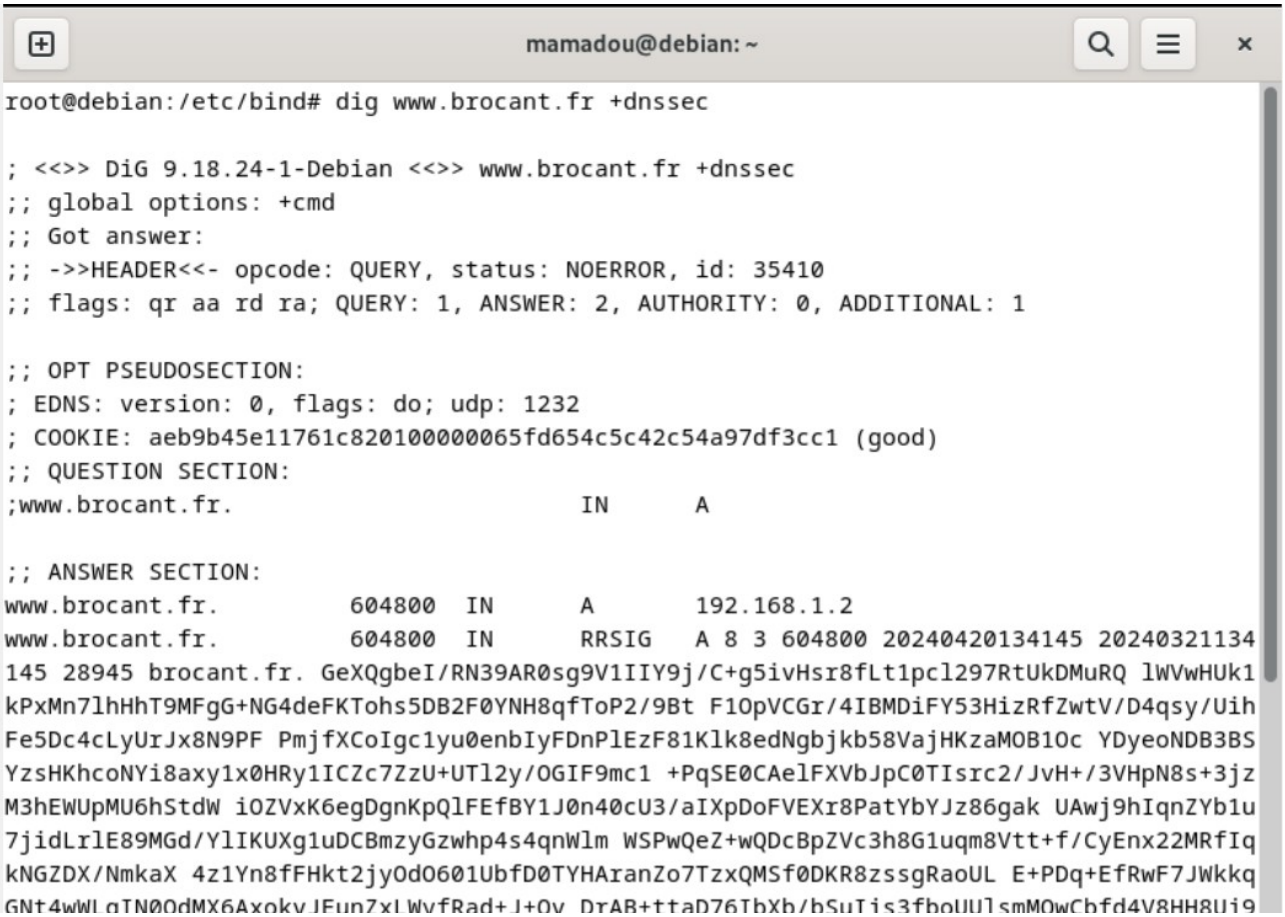
```
nano /etc/bind/named.conf.options
```

et dans le bloc options{}, on rajoute **dnssec-validation auto ;**
En suite, dans le fichier **named-conf.local**, on informe BIND de cette nouvelle zone signée en modifiant la directive « file » en précisant le chemin absolu du fichier signé pour les deux zone

```
 GNU nano 7.2                          named.conf.local

zone "brocant.fr" {
        type master;
        file "/var/cache/bind/db.brocant.fr.signed";
        allow-transfer { 192.168.1.100; };
        also-notify { 192.168.1.100; };
};



zone "1.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192.168.1.rev.signed";
        allow-transfer { 192.168.1.100; };
        notify yes;
};
// Consider adding the 1918 zones here, if they are not used in your
// organization
include "/etc/bind/zones.rfc1918";
```

Test de la configuration

dig www.brocant.fr +dnssec


mamadou@debian: ~
root@debian:/etc/bind# dig www.brocant.fr +dnssec
; <<>> DiG 9.18.24-1-Debian <<>> www.brocant.fr +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35410
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
; COOKIE: aeb9b45e11761c820100000065fd654c5c42c54a97df3cc1 (good)
;; QUESTION SECTION:
;www.brocant.fr. IN A
;; ANSWER SECTION:
www.brocant.fr. 604800 IN A 192.168.1.2
www.brocant.fr. 604800 IN RRSIG A 8 3 604800 20240420134145 20240321134
145 28945 brocant.fr. GeXQgbeI/RN39AR0sg9V1IIY9j/C+g5ivHsr8fLt1pcl297RtUkDMuRQ lWVwHUk1
kPxMn7lhHhT9MFgG+NG4deFKTohs5DB2F0YNH8qfToP2/9Bt F1OpVCGr/4IBMDiFY53HizRfZwtV/D4qsy/Uih
Fe5Dc4cLyUrJx8N9PF PmjfXCoIgc1yu0enbIyFDnPlEzF81Klk8edNgbjkb58VajHKzaMOB1Oc YDyeoNDB3BS
YzsHKhcoNYi8axy1x0HRy1ICZc7ZzU+UTl2y/OGIF9mc1 +PqSE0CAelFXVbJpC0TIsrc2/JvH+/3VHpN8s+3jz
M3hEWUpMU6hStdW iOZVxK6egDgnKpQlFEfBY1J0n40cU3/aIXpDoFVEXr8PatYbYJz86gak UAwj9hIqnZYb1u
7jidLrlE89MGd/YlIKUXg1uDCBmzyGzwhp4s4qnWlm WSPwQeZ+wQDcBpZVc3h8G1uqm8Vtt+f/CyEnx22MRfIq
kNGZDX/NmkaX 4z1Yn8fFHkt2jyOdO601UbfD0TYHAranZo7TzxQMSf0DKR8zssgRaoUL E+PDq+EfRwF7JWkkq
GNt4wWLgIN0OdMX6AxokvJEunZxLWyfRad+J+Oy DrAB+ttaD76IbXb/bSuIis3fboUUlsmMOwCbfd4V8HH8Ui9