

TSIG

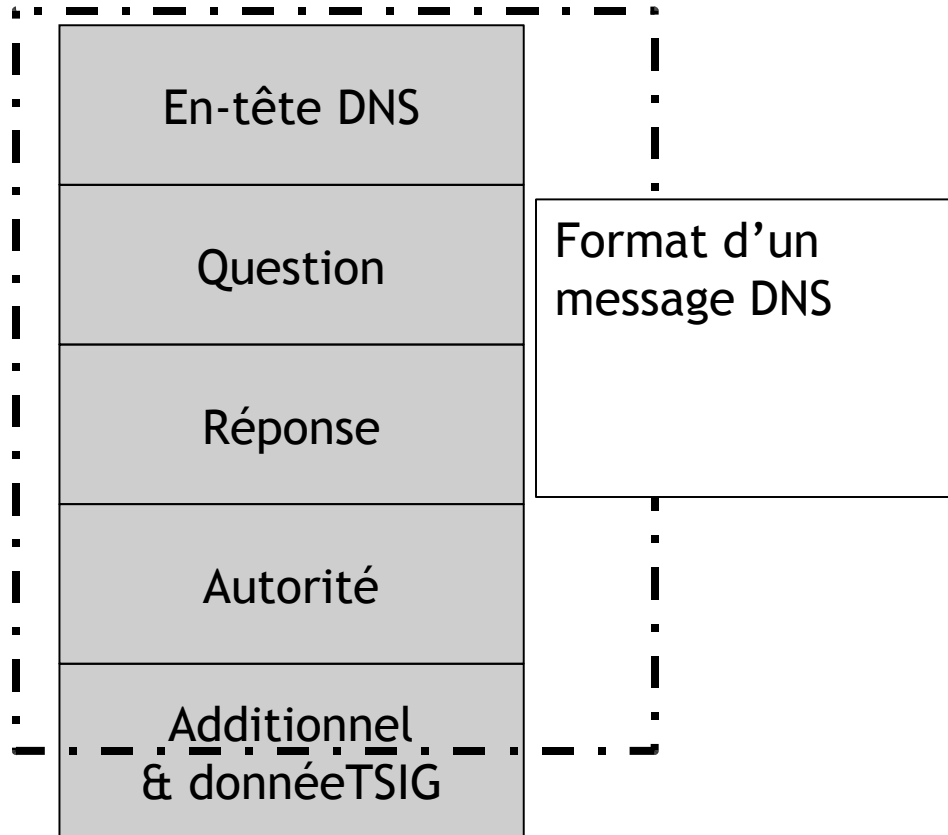
aalain@afrinic.net



Qu'est-ce que TSIG ?

- Un mécanisme pour protéger un message d'un résolveur au serveur et vice versa
- Un hash avec clé est appliqué(comme une signature digitale). Ainsi le destinataire peut vérifier le message
- Basé sur une valeur secrète partagée - expéditeur et destinataire sont configurés avec la valeur
- RFC2845

TSIG et format des messages



TSIG et format de message

```
;<<>> DiG 9.3.0 <<>> @localhost www.rfi.fr a -k /var/named/keys/Khost1-host2.+157+50032.key
```

```
:: QUESTION SECTION:
```

```
;www.rfi.fr.          IN      A
```

```
:: ANSWER SECTION:
```

```
www.rfi.fr.          86400  IN      A      194.117.210.38
```

```
:: AUTHORITY SECTION:
```

```
rfi.fr.              86400  IN      NS      ns1.mgn.net.
```

```
rfi.fr.              86400  IN      NS      ns2.mgn.net.
```

```
rfi.fr.              86400  IN      NS      ns3.mgn.net.
```

```
:: ADDITIONAL SECTION:
```

```
ns1.mgn.net.         172800 IN      A      195.46.193.86
```

```
ns2.mgn.net.         172800 IN      A      195.46.193.87
```

```
ns3.mgn.net.         172800 IN      A      195.46.214.178
```

```
:: TSIG PSEUDOSECTION:
```

```
host1-host2.         0      ANY    TSIG   hmac-md5.sig-alg.reg.int. 1126708829 300 16
```

```
jfqapw+5tnpqKceNaf5RnQ== 31634 NOERROR 0
```

```
; <<>> DiG 9.3.0 <<>> @localhost ripe.net a -k /var/named/keys/Khost1-host2.+157+50032.key +dnssec  
;; global options: printcmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39  
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 2
```

```
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags: do; udp: 4096  
;; QUESTION SECTION:  
;ripe.net. IN A
```

```
;; ANSWER SECTION:  
ripe.net. 592 IN A 193.0.0.214  
ripe.net. 592 IN RRSIG A 5 2 600 20051014125237 20050914125237 49526 ripe.net.  
GFWL87C+fcxPkFQ93ifF3SS0eq523Ktv92p0QPgCrs2q4t9pMVy8qjHN  
oTXEmthamwGdIy90wW5lcUtcfZMTarhx+0Q7zJwO76sXcjjNqMB4nbEb i2D/596k23DghZ/  
+Wg/zy/u0yRoYm0LfmbKIZE4WHnb7AeSadKjEz+Ts iuS5wdk5F7SkxginC2JfYRmgxQOQ9NaY
```

```
;; ADDITIONAL SECTION:  
ripe.net. 3592 IN DNSKEY 257 3 5  
AQOTT7bx7N38sPgDWniKnHnSnTxYxdMpEq7dyrDHDaRQgg7DULPWX6ZY  
0U1XKKMuNloHRP7H8r17IBhgXcPZjZhtSGYagtPe22mhAMjZ4e8KGgP9  
kJTtcpgzoYulvSiETBxjQ42EZWJG+6bXk+vyrwTbqEScmdZfqQz3ltVw  
k6Sos0UuSmTeb2C6RSkgHaTpKC5yIrnCVer1gvvyXGv3HOel8jiDGuj  
8peNByiaSRD4OIJUxu1jUqLvFDH6Anq6ZeNohxsYVUVajiRI1T+3x5+8  
acgwat3V55Z1Nm4O4Z1BKECdPO65EXIEC7/pqs5XvpsiJbafdj03uqLS a3aScpy3  
ripe.net. 3592 IN DNSKEY 256 3 5  
AQPgMhQPgNllavUXhVoDZZploCWbHr7lqcIGEiR/ct0KCTx4Skp+tBfX  
qnq8fz8/UpK4B+s6xIk5FPdjNnFXltdSx81bcM+BadLHL5iuBdQdkH8e  
yJq2Fk1LAUiP2AB8RAFbd4WQMAklw5z/91jw6aMXSfAo6sSxUFSS1WY8  
ChesKvwefNcqglSswlFwxjWHo9XNkFsx0u8=
```

```
;; TSIG PSEUDOSECTION:  
host1-host2. 0 ANY TSIG hmac-md5.sig-alg.reg.int. 1126710236 300 16  
eaDNJtJXavAjVqDZSA== 39 NOERROR 0
```

Nom et valeur secrète

- Nom TSIG
 - Un nom est donné à la clé, le nom est ce qui est transmis dans le message (ainsi le destinataire sait quelle clé l'expéditeur a utilisé)
- Valeur secrète TSIG
 - Une valeur déterminée pendant la production de la clé
 - Généralement codée en Base64
- Ressemble à la clé rndc
 - BIND utilise la même interface pour les clés TSIG et RNDC



Utilisation de TSIG pour protéger AXFR

- Détermination de la valeur secrète
 - `dnssec-keygen -a ... -b ... -n... name`
- Configuration de la clé
 - dans `named.conf`, même syntaxe que `rndc`
 - `key { algorithm ...; secret ...;}`
- Utilisation de la clé
 - Dans `named.conf`
 - `server x { keys ...; }`
 - Où 'x' est l'adresse IP des autres serveurs

Exemple de configuration

Serveur primaire

10.33.40.46

```
key ns1-ns2.zone. {
    algorithm hmac-md5;
    secret "APlaceToBe";
};
server 10.33.40.35 {
    keys {ns1-ns2.zone.;;};
};
zone "my.zone.test." {
    type master;
    file...;
    allow-transfer {
        key ns1-ns2.zone.;
        key ns1-ns3.zone.;;};
};
```

Serveur secondaire

10.33.40.35

```
key ns1-ns2.zone. {
    algorithm hmac-md5;
    secret "APlaceToBe";
};
server 10.33.40.46 {
    keys {ns1-ns2.zone.;;};
};
zone "my.zone.test." {
    type slave;
    file...;
    masters {10.33.40.46;};
    allow-transfer {
        key ns1-ns2.zone.;;};
};
```

Une fois encore, la valeur secrète semble ok, mais est invalide

Le temps!!!

- TSIG est sensible au temps - pour arrêter les « attaques de retransmission »
 - La protection des messages expire en 5 minutes
 - S'assurer que les horloges sont synchronisées
 - Pour les tests, régler les horloges
 - En production, un NTP sécurisé est nécessaire

Autres utilisations de TSIG

- TSIG était conçu pour d'autres objectifs
 - Protection des “stub resolvers” sensibles
 - Difficile à réaliser
 - Les mises à jour dynamiques
 - Leur sécurisation dépend du TSIG