Projet fédérateur G6-DNSSEC

Date : 21 nov. 2002
Auteurs : Nicolas Notari, Jean-Philippe Pick, Mohsen Souissi
E-Mails : {Nicolas.Notari, Jean-Philippe.Pick, Mohsen.Souissi, g6-dnssec}@nic.fr
Version : 2.2

I. Introduction

La sécurisation du DNS (DNSSEC) peut être considérée sur deux plans :

- Sécurisation de la communication entre deux serveurs avec TSIG au moyen d'un secret partagé (cryptographie symétrique):
  - transferts de zones entre un master et un slave ou entre 2 slaves,
  - mise à jour dynamique (Dynamic Update) vers un master depuis d'autres serveurs (DHCP, ...),
  - requêtes et réponses entre 2 serveurs (par exemple entre 2 serveurs récursifs locaux (caches),...)

- Sécurisation des messages échangés entre clients et serveurs DNS (requêtes et réponses). On s'appuie ici sur la cryptographie asymétrique en utilisant un système de clef publique/clef privée. La mise en oeuvre de cette partie nécessite la prise en compte d'aspects techniques et administratifs par tous les acteurs souhaitant participer au projet.

Dans les 2 cas TSIG et DNSSEC proposent un service de signature (authentification et intégrité), mais ne proposent pas de service de chiffrement pour le transport des données DNS. Il est à noter que l'utilisation de cette sécurisation ne préserve pas des attaques de type « Déni de Service ».

Des propositions de projet fédérateur DNSSEC ont déjà été diffusées sur la liste du G6. Celles-ci ont été discutées et convergent vers une solution qui semble satisfaire tous les critères du projet. Cela sera dans un espace dédié sous le 2001:0660:F100::/40 et TOUT LE MONDE Y A DROIT. Voici le détail de l'architecture.

Deux modèles de chaîne de confiance non inter opérables sont disponibles (RFC 2535 et Draft-DS[1]). Le modèle proposé dans la Draft DS est à utiliser pour ce projet (depuis la version 2.0 de ce document).

L'objectif dans un premier temps du projet DNSSEC sera de tester la délégation, la signature et le transport sécurisé des requêtes et des réponses DNS... Cela dit, Renater n'aura pas à assurer la connectivite pour ces adresses de test. Autrement dit, que l'on soit agrée Renater ou pas, on n'aura pas de connectivité IPv6 pour ces préfixes DNSSEC. Mieux encore, il n'y aura pas de numérotation réelle des sites/machines avec ces préfixes. Le fichier de zone pourra être rempli par des noms complètement virtuels. En un mot, le projet DNSSEC pourra être entièrement découplé du routage et de tout trafic réel.

Plus concrètement, voici le découpage proposé en partant de la racine (préfixe 2001:660:F100::/40 de Renater) :

- un préfixe particulier, le 2001:660:F100::/40 est déclaré "sommet de l'arbre reverse DNSSEC". Renater délègue la gestion l'arbre en question à l'AFNIC qui lui associe une clef. Cette dernière qui sera considérée comme une clef de confiance ("trusted key") à tous les niveaux inférieurs de la hiérarchie, sera signée par elle-même (auto signature) ;

- l'AFNIC ou « RootSec » alloue jusqu'a 16 préfixes de la forme 2001:660:F1x0::/44 aux PIRSec en leur déléguant les zones reverses correspondantes selon le plan d'adressage spécifié à l'annexe A ;

- chaque PIRSec construit sa propre clef qui sera auto signée, qui sera référencée dans la zone parente « RootSec », et qui servira à prolonger la chaîne de confiance ;

[1] http://www.ietf.org/internet-drafts/draft-ietf-dnsext-delegation-signer-11.txt

- chaque PIRSec assigne jusqu'à 16 blocs à des "SiteSec" (sites sécurisés) de la forme 2001:660:F1xy::/48 selon un plan d'adressage qu'il détermine ; les zones reverses correspondantes sont alors déléguées au client ;

- chaque SiteSec client construit sa propre clef qui sera auto signée, qui sera référencée dans la zone parente (celle du PIRSec au-dessus) et qui servira à prolonger la chaîne de confiance ;

- chaque site pourra découper son /48 en sous-réseaux et faire la délégation et la signature en suivant le schéma hiérarchique qui vient d'être décrit ;

Ainsi, nous essaierons de suivre la topologie du pilote IPv6 de Renater2 pour structurer les délégations DNSSEC. Les PIRSec intéressés par le projet s'adresseront à l'AFNIC opérant le « RootSec » pour demander la délégation de leur zone DNSSEC. Les sites intéressés ayant déjà un /48 sous 3ffe ou 2001 s'adresseront au PIRSec le plus proche pour leur déléguer une zone DNSSEC.

Ce projet dans ses versions 1.x proposait un déploiement dans l'arbre ip6.int en suivant le schéma de la RFC 2535. A partir de cette version 2.x nous proposons d'abandonner l'ancien arbre et de recommencer un déploiement sous ip6.arpa en suivant le schéma proposé par la Draft DS.

Pour ceux qui ne sont pas familiers avec DNSSEC, il existe une présentation réalisée par l'AFNIC à l'école thématique vCARS 2002 (accessible à partir de l'URL http://www.urec.cnrs.fr/securite/CNRS/vCARS/DOCUMENTS/Notari.pdf) et des supports de cours et présentations faits par le groupe DISI de RIPE (accessibles à partir de l'URL http://www.ripe.net/disi/).

Si toutefois, certaines choses vous paraissent peu claires nous restons à votre disposition à l'adresse email g6-dnssec@nic.fr .

II. Hypothèses et remarques

Nous nous proposons de démarrer le déploiement de DNSSEC selon les démarches qui suivent. Ces démarches s'appuient sur certaines restrictions qui devraient faciliter le lancement du projet. Les procédures ne sont pas définitives car des propositions en cours peuvent apporter des améliorations importantes aux standards proposés actuellement (notamment Draft-DS, RFC 2535, RFC 2845, RFC 3008, et RFC 3090).

II.1. Remarques

On suppose que toute le monde utilise le logiciel bind version 9.3.x minimum disponible à l'URL ftp://ftp.isc.org/isc/bind9 (la dernière version disponible à l'heure de l'écriture de ce document est la version 9.3.0s20020722 incluse dans le sous répertoire /snapshots). Nous rappelons que l'utilisation de versions snapshots peut engendrer des problèmes de stabilité : on évitera donc d'utiliser ces versions pour des domaines utilisés en « production ».

II.2. Terminologie

On spécifie ici un résumé de la terminologie utilisée dans un but de référence. La signification de certains éléments s'éclaircira à la lecture de la suite du document.

- un keyset est un fichier « trousseau » de clef(s) publique(s) au format RR (Resource Record) KEY qui est destiné à être envoyé au parent pour référencement dans sa zone de la clef utilisée pour le chaînage de confiance. Il ne s'agit plus de l'intégralité du RRset KEY et il ne figure plus de signatures sous forme de RR SIG dans ce fichier (cf RFC 2535)

Les commandes apparaissent dans une police réservée (`command`) :

- les commandes shell précédées d'un $ sont à lancer en tant qu'utilisateur
- les commandes shell précédées d'un # sont à lancer en tant que root

Un certains nombre d'alias apparaissant en italique sont utilisés pour alléger le document :

- soit *$zone* le nom de votre zone à utiliser pour le projet
- soit *$source_zone_file* le fichier de zone que vous allez créer (avant sécurisation)
- soit *$prefixe_pirsec* le chiffre hexadécimal désignant le PIRSec dans $zone
- soit *$prefixe_local* le chiffre hexadécimal désignant le SiteSec dans $zone
- soit *$clef_chaîne* la clef (et le nom correspondant aux fichiers de la clef) utilisée pour la chaîne de confiance
- soit *$clef_locale* la clef (et le nom correspondant aux fichiers de la clef) utilisée pour signer votre zone (si vous décidez d'en générer une).
- Soit *$durée_signature* la durée en seconde de la signature par rapport à l'instant de la signature

I.3. Conseils

Nous vous conseillons de travailler dans un autre endroit que là où se trouvent les fichiers de zone de bind, non seulement pour d'évidentes raison de sécurité, mais aussi pour ne pas polluer le répertoire où doivent se trouver uniquement des fichiers de zone.

III. Procédures

III.1. Demande de délégation sous l'arbre 1.f.0.6.6.0.1.0.0.2.ip6.arpa

III.1.1. Déterminer le nom de zone et la configurer

Pour déterminer le nom de la zone que vous devez configurer :

- Si vous êtes un PIRSec, référez-vous à l'annexe A pour connaître la valeur de votre *$prefixe_pirsec*. La zone à configurer est alors *$prefixe_pirsec*.1.f.0.6.6.0.1.0.0.2.ip6.arpa.

- Si vous êtes un SiteSec, contactez votre PIR pour exprimer votre intention de participer au projet. Il vous attribuera un *$prefix_sitesec* (sous la forme d'un chiffre hexadécimal qu'il choisira selon sa propre politique d'attribution). Référez-vous à l'annexe A pour connaître la valeur du *$prefixe_pirsec* correspondant à votre PIR. La zone à configurer est alors *$zone=$prefixe_sitesec.$prefixe_pirsec*.1.f.0.6.6.0.1.0.0.2.ip6.arpa

Pour configurer la zone :

- Si vous disposez de deux serveurs de nom au minimum utilisant une version de bind 9.3.x ou supérieure :

- configurez alors ces serveurs de nom pour qu'ils fassent autorité pour *$zone*. Il n'est pas indispensable que ces serveurs disposent d'une connectivité IPv6 mais ils doivent dans tous les cas disposer d'une connectivité IPv4.
- Il est possible d'utiliser TSIG pour réaliser les transferts entre serveurs maître et esclave (voir exemple en Annexe B)

- Si vous ne disposez que d'un serveur de nom utilisant une version de bind 9.3.x ou supérieure :

  - Configurez alors ce serveur de nom pour qu'il fasse autorité pour *$zone*.Il n'est pas indispensable que ce serveur dispose d'une connectivité IPv6 mais il doit dans tous les cas disposer d'une connectivité IPv4.
  - Envoyer un mail à `g6-dnssec@nic.fr` en précisant votre statut, le PIR dont vous dépendez si vous êtes un site et votre souhait d'obtenir un service de nom secondaire. Jusque là, l'AFNIC a offert un service de secondaire sur ns3.nic.fr. Ce dernier serveur tourne un serveur BIND 9.2.1 en production et ne pourra donc pas participer au projet fédérateur sous BIND 9.3.x. L'AFNIC met en place un nouveau serveur secondaire, ulysse.nic.fr, qui pourra vous être fourni dans le cadre de ce projet à la place de ns3.nic.fr. Précisez également si vous souhaitez utiliser TSIG (voir Annexe B), auquel cas une clef TSIG et son nom de clef vous seront envoyés en retour.
  - Si vous avez choisi d'utiliser TSIG, autorisez la clef TSIG de l'AFNIC pour que le serveur ulysse.nic.fr puisse effectuer des transferts de zones (AXFR) pour *$zone* à partir de votre serveur (voir Annexe B).
  - Incluez dans *$zone* une ligne « IN NS ulysse.nic.fr.» en dessous du RR NS déjà existant correspondant à votre serveur.
  - Renvoyez un mail à `g6-dnssec@nic.fr` en indiquant que la configuration est terminée de votre côté et en précisant *$zone* et l'adresse IPv4 de votre serveur de nom (ainsi que l'adresse IPv6 s'il en dispose d'une).

III.2. Génération de clef(s) & signature de la zone

III.2.1. Durée et fréquence de signature

Si vous êtes un SiteSec et que vous ne faites pas figurer de délégation dans votre zone sécurisée, l'AFNIC recommande une durée de signature longue (par exemple 6 mois). En effet le PIRSec qui gère la zone parente de la vôtre re-signera très fréquemment sa zone (et donc le DS RRset qui vous correspond). En cas de compromission de votre (vos) clef(s) utilisée(s) pour la chaîne de confiance, vous pourrez contacter votre PIRSec et l'intervalle de vulnérabilité se limitera à la durée restante de la dernière signature de la zone parente gérée par le PIRSec. Pour éviter une expiration des signatures dans votre zone due à un oubli, prévoyez sur votre planning une re-signature quelques temps avant la date d'expiration.

Si vous êtes un PIRSec une durée de signature brève et une importante fréquence de re-signature est nécessaire pour les raisons exposées précédemment. Quoi qu'il en soit, il faudra impérativement éviter qu'à un instant donné les seules signatures disponibles dans votre zone soient des signatures expirées.

Les PIRSec désirants par exemple signer leur zone tous les jours pourront mettre en place un script lancé par le démon crond automatisant :

- l'incrémentation du numéro de série de la zone (avant chaque re-signature)
- la signature (voir `dnssec-signzone` plus bas),
- le rechargement du serveur (`rndc reload`).

À titre préventif (la fréquente signature de leur zone par les PIRSec pourrait l'en dispenser), le « RootSec » opéré par l'AFNIC sera dans un proche futur automatiquement re-signé tous les jours avec une durée de signature courte.

Il est important de noter que durée de signature et TTL ne sont pas décorrélés. En effet, la durée de vie dans un cache d'un RRset obtenu à un instant donné est le minimum du TTL et de la durée de vie restante de la signature.

Dans la suite de ce document *$durée_signature* représente la durée en secondes de cette signature par rapport à l'instant de signature.

III.2.2 Nombre de clefs

On utilise ici le chiffrement asymétrique et donc des paires de clefs correspondantes : clef publique/clef privée

Deux solutions s'offrent à vous :

- Générer plusieurs paires de clefs (au moins 2) dont au moins une sera utilisée uniquement pour la chaîne de confiance (pour des raisons de performances dans le cadre de ce projet on se limitera au maximum à une clef pour la chaîne de confiance afin de limiter à un seul RR la taille dans la zone parente du RRset DS pour une zone fille donnée). On parle de « clef signant les clefs » ("key signing key").
  Ce n'est pas la paire de clefs utilisée pour la chaîne de confiance (et donc la paire de clé dont la clé publique est référencée par le DS dans la zone parente) qui sera utilisée pour signer toute votre zone. Vous limitez ainsi la quantité de données signées avec la clé privée appartenant à la paire de clefs utilisée pour la chaîne de confiance, limitant du même coup d'autant le matériel pouvant être utilisé pour une attaque. La paire de clefs utilisée pour la chaîne de confiance et dont la clé publique est référencée dans la zone parente n'est utilisée que pour signer le RRset KEY au sommet de votre zone.
  La clef que vous utiliserez pour signer la zone peut alors être changée à convenance, selon votre politique, sans devoir reprendre contact avec la zone parente.
  Cette solution est la solution recommandée par l'AFNIC.

- Générer une paire de clefs unique qui servira pour la chaîne de confiance et pour signer votre zone.

Notez que dans les deux cas vous pouvez inclure des clefs destinées à un autre usage dans le RRset KEY au sommet de votre zone sans nécessité de contacter votre zone parente.

III.2.3. Signature multi-clefs (multi-paires)

III.2.3.a. Génération des paires de clefs

Générez une paire de clef à utiliser pour la chaîne de confiance en procédant comme suit :

```
$ dnssec-keygen -a RSASHA1 -b 1024 -n ZONE $zone
```

L'option -a correspond à l'algorithme de génération de la clef
L'option -b correspond à la taille de cette clef

Exemple en se plaçant dans le cas *$prefixe_pirsec*=0 et *$prefixe_sitesec*=0:

```
$ dnssec-keygen -a RSASHA1 -b 1024 -n ZONE 0.0.1.f.0.6.6.0.1.0.0.2.ip6.arpa.
```

➔ on obtient deux fichiers *$clef_chaîne*.key et *$clef_chaîne*.private
(avec dans ce cas *$clef_chaîne*= K.0.0.1.f.0.6.6.0.1.0.0.2.ip6.arpa.+001+29679) :

K.0.0.1.f.0.6.6.0.1.0.0.2.ip6.arpa.+001+29679.key, correspondant à la partie publique de la clef
K0.0.1.f.0.6.6.0.1.0.0.2.ip6.arpa.+001+29679.private, correspondant à la partie privée de la clef.

Répétez l'opération de la même manière pour obtenir votre seconde paire de clefs (fichiers *$clef_locale*.key et *$clef_locale*.private)

III.2.3.b Signature de la zone

Signez votre zone en procédant comme suit :

- Déposez tous les fichiers de clefs générés précédemment dans le même répertoire que votre zone

- Incluez les clefs publiques de vos paires de clefs dans votre fichier de zone *$source_zone_file* en ajoutant dans le fichier les lignes :
  $INCLUDE *$clef_chaîne*.key
  $INCLUDE *$clef_locale*.key

- Augmentez le serial de votre zone dans le fichier de zone *$source_zone_file* complet si vous l'aviez déjà chargé dans votre bind.

- Déposez tous les fichiers au format keyset-*[nom_de_zone_fille]* que vous avez reçu de la part des zones filles (s'il y en a), dans le même répertoire que votre zone.

- Signez votre zone :

```
$ dnssec-signzone -o $zone –e +$duree_signature -k $clef_chaine.private
   -f $zone.signed $source_zone_file $clef_locale.private
```

Par exemple :

```
$ dnssec-signzone –o 0.0.1.f.0.6.6.0.1.0.0.2.ip6.arpa.
   -e +15000000
   –k K1.f.0.6.6.0.1.0.0.2.ip6.arpa.+001+29679.private
   -f 0.0.1.f.0.6.6.0.1.0.0.2.ip6.arpa.signed
   0.0.1.f.0.6.6.0.1.0.0.2.ip6.arpa
   K1.f.0.6.6.0.1.0.0.2.ip6.arpa.+001+87634.private
```

Résultat obtenu :

- Le fichier de zone auquel a été rajouté les RR de types NXT, SIG, DS nécessaires est généré sous le nom *$zone*.signed ou un autre nom que vous aurez choisi avec –f.

- Un fichier au format keyset-*[nom_de_votre_zone]* à conserver pour envoyer à la zone parente est automatiquement ajouté dans le répertoire dans lequel a eu lieu la signature.

III.2.4 Signature mono-clef (mono-paire)

III.2.4.a Génération de la paire de clefs

Procédez comme au III.2.3.a mais en vous limitant à la production d'une seule paire de clefs :

$clef_chaîne.key et *$clef_chaîne*.private.

III.2.4.b Signature de la zone

On procède comme au III.2.3.b mais en signant toute la zone avec *$clef_chaîne*.private.

Pour cela on inclut uniquement la clef publique *$clef_chaîne*.key dans la zone :

$INCLUDE *$clef_chaîne*.key

et on ne spécifie pas de clefs à `dnssec-signzone` :

```
$ dnssec-signzone -o $zone –e +$duree_signature
   -f $zone.signed $source_zone_file
```

Le reste de la marche à suivre reste inchangé.

III.3 Demande de délégation et envoi de clefs publiques au parent

- Le fichier *$zone*.signed (ou autre) obtenu peut être chargé dans votre master

- Contacter votre PIRSec si vous êtes un SiteSec ou l'AFNIC (g6-dnssec@nic.fr) si vous êtes un PIRSec pour demander la délégation de votre zone en précisant la liste des serveur de nom et en attachant au mail le fichier keyset-*[nom_de_votre_zone]* automatiquement produit par dnssec-signzone au III.2.3 ou III.2.4. Notez que le fichier keyset-*[nom_de_votre_zone]* convient pour la création du RRset DS (transmission de la clef utilisée pour la chaîne de confiance) dans la zone parente quelque soit la méthode de signature choisie (III.2.3 ou III.2.4).

- Chaque modification nécessite de repartir du fichier de zone original et de recommencer la procédure de signature (mais pas l'envoi du keyset à la zone parente tant que la paire de clef utilisée pour la chaîne de confiance ne change pas)

IV. Conclusion

Nous comptons démarrer le projet avec les hypothèses et démarches décrites ci-dessus. Celles-ci peuvent être amenées à changer en fonction du retour d'expérience des différents acteurs du projet et de l'évolution des standards DNSSEC. Tous vos commentaires, critiques et suggestions seront les bienvenus à l'adresse g6-dnssec@nic.fr.

V. Annexes

Annexe A : Plan de numérotation des PIRSecs

Le préfixe *$préfixe_pirsec* est un unique chiffre qui est la représentation hexadécimale du mot binaire constitué de la séquence du 38ème au 41ème bit (inclus) du préfixe IPv6 /41 utilisé par le PIR dans le pilote IPv6 de Renater 2.

Ainsi on a :

PIRSec	Zone
Ile de France	2.1.f.0.6.6.0.1.0.0.2.ip6.arpa
Grenoble	3.1.f.0.6.6.0.1.0.0.2.ip6.arpa
Strasbourg	4.1.f.0.6.6.0.1.0.0.2.ip6.arpa
Rennes	5.1.f.0.6.6.0.1.0.0.2.ip6.arpa
Nancy	6.1.f.0.6.6.0.1.0.0.2.ip6.arpa
Nice/Sophia-Antipolis	7.1.f.0.6.6.0.1.0.0.2.ip6.arpa
Toulouse	8.1.f.0.6.6.0.1.0.0.2.ip6.arpa

Annexe B : Exemple Utilisation de TSIG pour les transferts de zone

On utilise de la cryptographie symétrique. On utilise donc un secret partagé entre le master et au moins l'un des slaves.

L'outil dnssec-keygen peut être utilisé pour générer le secret partagé avec l'algorithme HMAC-MD5 comme dans l'exemple suivant:

```
$ dnssec-keygen -a HMAC-MD5 -b 512 –n HOST host1.domain.tld1.
```

On récupère le secret:

```
$ more Khost1.domain.tld1.+157+50758.private
  Private-key-format: v1.2
  Algorithm: 157 (HMAC_MD5)
 Key: 7TaW+MOJasc9yK9QRidNyP6pI/vxvZczEbsxGSYNfgFHGuTXnI1PqJfkNOu8xMkIjx6QjoQm/GvCkUU0VmSRdw==
```

Et on le met dans named.conf sur le master:

```
key “[nom_du_master]-[nom_du_slave]" {
   algorithm hmac-md5;
     secret "7TaW+MOJasc9yK9QRidNyP6pI/vxvZczEbsxGSYNfgFHGuTXnI1PqJfkNOu8xMkIjx6QjoQm/GvCkUU0VmSRdw==”
};

zone confiance.fr {
      type master;
      file “0.0.1.f.0.6.6.0.1.0.0.2.ip6.arpa”;
      allow-transfer { key [nom_du_master]-[nom_du_slave]; };
}
```

Et dans named.conf sur le slave :

```
key “[nom_du_master]-[nom_du_slave]" {
      algorithm hmac-md5;
      secret "7TaW+MOJasc9yK9QRidNyP6pI/vxvZczEbsxGSYNfgFHGuTXnI1PqJfkNOu8xMkIjx6QjoQm/GvCkUU0VmSRdw==”
}

server 192.249.249.1 {
      keys { [nom_du_master]-[nom_du_slave]; };
};

zone confiance.fr {
      type slave;
      file “0.0.1.f.0.6.6.0.1.0.0.2.ip6.arpa”;
      masters { 192.249.249.1; };
};
```

Il convient de remplacer *[nom_du_master]* et *[nom_du_slave]* par leur nom respectif et de former un nom de clef sans espace. Il est important que ce nom soit identique sur le master et sur le slave (il ne s’agit dans ce cas pas d’un nom local).

Remarque : Afin de garder la clef TSIG confidentielle, on essayera dans la mesure du possible d’éviter de faire figurer explicitement le secret dans le fichier named.conf et on préférera le faire figurer dans un fichier séparé en s’aidant de l’instruction `include`.

Annexe C : Outil de déboguage

La distribution BIND est livrée avec des outils de déboguage DNS, tels que host, nslookup et dig. Ce dernier est de loin le plus complet. En outre, ‘dig’ se prête bien à la vérification DNSsec et TSIG s’il est accompagné des arguments qu’il faut. Ainsi la commande ‘dig … +dnssec’ active le support de DNSsec pour la commande ‘dig’ en question. De même, la commande ‘dig –y <nom-de-la-clef-tsig> :<clef-tsig> @<serveur-partageant-le-secret> …’ permet de s’authentifier à la volée auprès du serveur au moment de la requête.

Exemple : regardez ce que donne la commande suivante :
‘dig @cyclope.ipv6.nic.fr 1.f.0.6.6.0.1.0.0.2.ip6.arpa SOA +dnssec’

Enfin, pour de plus amples informations, tapez tout simplement ‘man dig’ ;-)

Annexe D : Clef de confiance

La clef de confiance sert à annoncer l'entrée dans une arborescence DNSSEC. Elle indique le début d'une chaîne de confiance père-->fils à partir d'un certain noeud DNS. Dans notre cas, on considère que l'arbre DNS dont le sommet (« RootSec ») est 1.f.0.6.6.0.1.0.0.2.ip6.arpa sera sécurisé. Par conséquent, on pourra vérifier le fait qu'une zone sous cet arbre soit sécurisée en parcourant la chaîne de confiance à partir du sommet de cet arbre.

La clef de confiance peut être obtenue sous forme d'un fichier sous simple demande à `g6-dnssec@nic.fr` . C'est une clef de type RSASHA1 de longueur 2048 bits.

Cette clef de confiance (nouvelle version) devra être intégrée dans votre serveur de nom récursif local (cache) :

- Editez le fichier de configuration (named.conf) de votre serveur récursif local en y ajoutant la directive suivante :

```
trusted-keys {
      1.f.0.6.6.0.1.0.0.2.ip6.arpa. 256 3 5
      "AQOheAWMpTziH4v4gbMgSH6Q0C6rNkCRAivkk/cADOVSm/zHLYLfM/cj
       55/+eG88bzlsDZ2UqwEvhhslyWQ5jhGBuW6fy1rpwGnp9qclf6UWgBBg
       DCn6OX4zcTvWoAn5oX1/vCZ2YQgI8nS+qf4HnPvTPjhdsl3k3RnZyhNz
       5T+3CIy7E+fMbTDwo77kSd544q+h1LXzgbNAasyAUz/N62jKC2z6bXTP
       lQcNagkoL5+HMYK79OGx1VRQxR3oaTjr+H7qJfwzldytAqLvoq0dDaK0
       bZkj2+3j4B8xBA/C6+XboqwwruV3hFl+oyOnzfTM5VC99+yu2x8ouyXg
       wphLKevn";
};
```

- Rechargez votre serveur pour relire la nouvelle configuration (`rndc reload`).

Remarque : La vérification étant pratiquée par le serveur récursif lors de la résolution du nom, la présence de trusted-keys pour cette clef sur des serveurs non récursifs même s'ils font autorité pour une zone sécurisée n'est pas nécessaire.