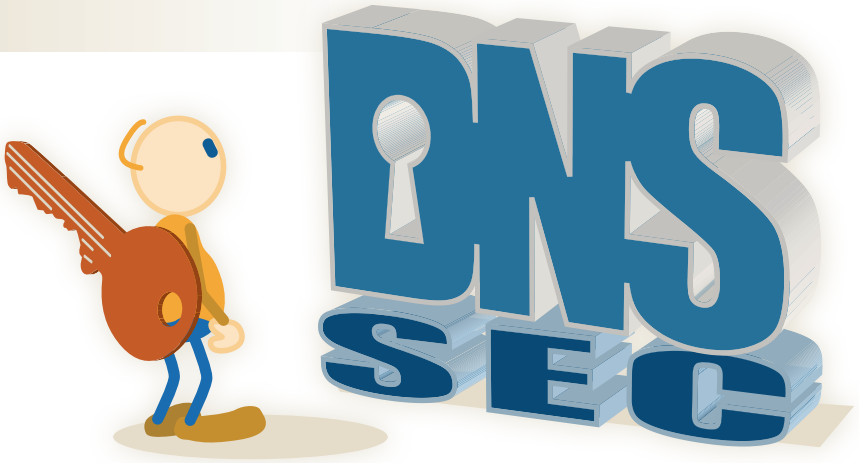
DNSSEC

les extensions de sécurité du DNS



Introduction

Enjeux de DNSSEC

La sécurité de tout système dépend à la fois de la sécurisation de ses différentes composantes et des interactions entre celles-ci. Ce constat est aussi valable pour le DNS (Domain Name System), maillon clé du fonctionnement de l'Internet, car la quasi-totalité des services en ligne utilise des noms de domaine à un moment ou à un autre. Cependant, le DNS a été mis au point dans les années 80, dans un environnement où sa capacité à répondre aux besoins de performance et de résilience primait sur sa sécurisation. Avec le temps, et notamment depuis 2008, avec la révélation de la « Faille Kaminsky », la nécessité de mieux sécuriser le DNS est devenue une priorité pour tous ses acteurs.

S'il ne saurait répondre à l'ensemble des attaques possibles contre le DNS, le protocole DNSSEC permet d'apporter une protection durable – et demain, indispensable – contre les agressions dites « par empoisonnement de cache » visant à substituer de fausses informations aux vraies dans le processus de résolution des noms de domaine. L'attaquant peut ainsi espérer leurrer des utilisateurs et les détourner vers son site à leur insu. Or la capacité croissante des machines et du réseau en termes de débit rend désormais possible des attaques qui, jusqu'à présent, n'étaient que théoriques, compte tenu de leur faible probabilité de succès.

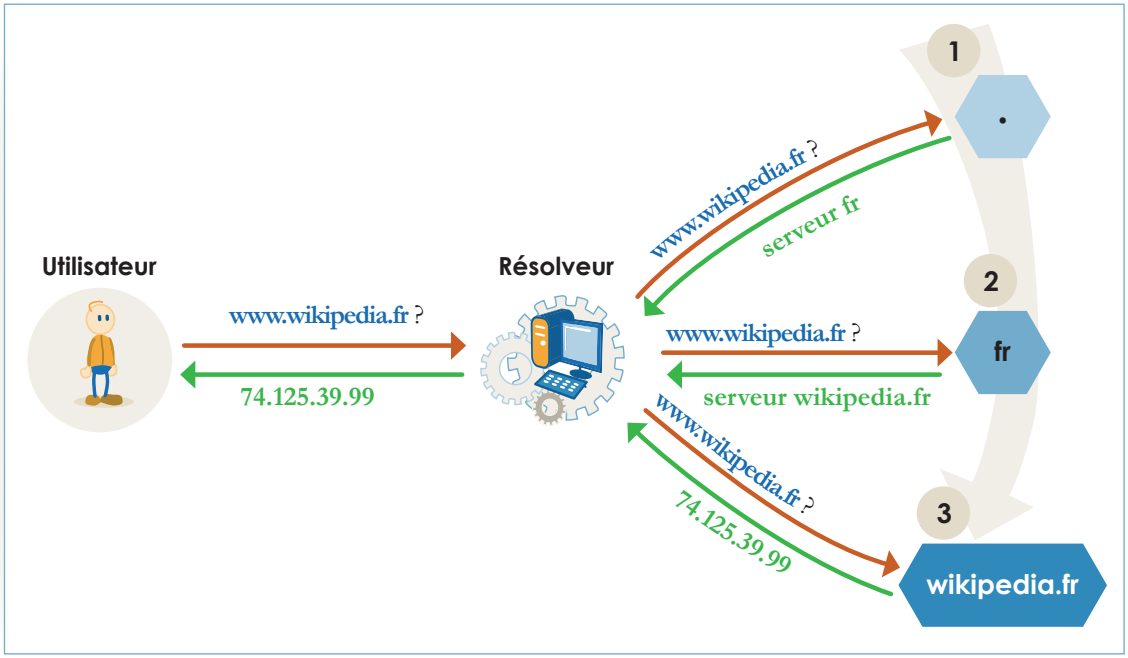
Le présent dossier thématique s'inscrit dans la continuité de celui que l'AFNIC a déjà consacré à la sécurité du DNS[1], en explorant plus précisément les tenants et les aboutissants de DNSSEC. Il a pour objectif d'apporter des éléments de compréhension de ses enjeux et de son fonctionnement, afin de permettre au lecteur de mieux s'approprier cette évolution qui va modifier la physionomie du DNS dans les années à venir.

[1] www.afnic.fr/data/divers/public/afnic-dossier-dns-attaques-securite-2009-06.pdf

1 Organisation et fonctionnement du DNS

Le DNS est organisé sous la forme d'une arborescence inversée, avec une « racine » dont dépendent les différentes « branches ». Au premier niveau de l'arborescence se trouvent les « Top Level Domains » ou domaines de premier niveau, comme les *.fr*, *.com* etc. Au second niveau, nous avons les noms de domaine « classiques » comme « afnic.fr ».

Fonctionnant comme une base de données distribuée sur des millions de machines, le DNS repose sur des interactions entre ces machines permettant d'identifier celle qui est la plus susceptible de pouvoir répondre à la requête d'un internaute.



La résolution DNS

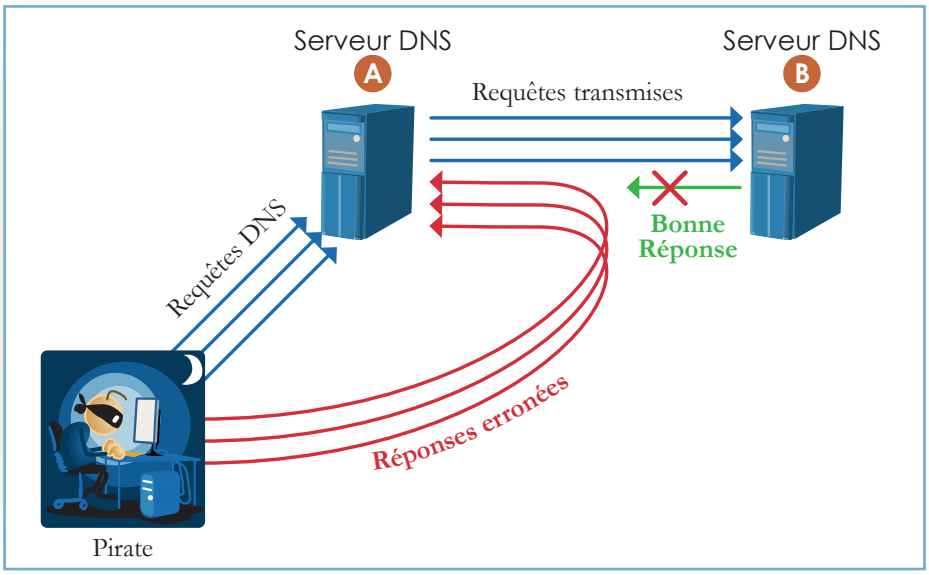
Dans l'exemple ci-dessus, l'utilisateur veut se connecter au site http://www.wikipedia.fr. Il envoie sa requête via son navigateur. Celle-ci est reçue par un serveur dit « résolveur » qui a pour première mission d'identifier la machine sur laquelle est installé le nom de domaine wikipedia.fr. Le résolveur s'adresse d'abord à la « racine » du DNS, qui lui indique quelles sont les serveurs « faisant autorité » (c'est-à-dire compétents) pour *.fr* puisque le nom de domaine est en *.fr*. Dans un second temps, les serveurs du *.fr* indiquent à leur tour au résolveur que le nom de domaine wikipedia.fr est hébergé sur tel serveur. Celui-ci est alors en mesure d'indiquer au navigateur l'adresse IP du serveur web hébergeant les contenus du site web www.wikipedia.fr.

Ce schéma est vrai quel que soit le site web auquel on souhaite accéder, et quelle que soit l'adresse électronique à laquelle on souhaite écrire.

2 Les attaques par empoisonnement de cache

Le dossier thématique de l'AFNIC consacré à la sécurité du DNS dresse un panorama des grands types d'attaques possibles, depuis les attaques ne visant pas directement le DNS (cybersquatting, vol de noms de domaine…) jusqu'à celles qui se concentrent sur lui, telles les attaques par déni de services ou empoisonnement de cache.

DNSSEC répond spécifiquement aux attaques par empoisonnement de cache visant à intoxiquer le « résolveur » pour qu'il considère que le serveur « pirate » est légitime, en lieu et place du serveur originel. Cette opération permet notamment de capter et de détourner les requêtes vers un autre site web sans que les utilisateurs puissent s'en rendre compte, avec à la clé le risque de les voir confier des données personnelles en se croyant sur le site légitime de la victime de l'attaque.



Les attaques par empoisonnement de cache

Le bon fonctionnement du DNS dépend donc étroitement de la fiabilité des données transmises à chaque étape. Les extensions de sécurité du DNS cherchent à répondre à cette contrainte en assurant l'intégrité des données transitant sur le réseau, notamment entre résolveurs et serveurs faisant autorité.

3 Qu'est-ce que DNSSEC ?

DNSSEC est l'acronyme de Domain Name System Security Extensions, il désigne un ensemble défini d'extensions de sécurité du protocole DNS.

Ces extensions utilisent les mécanismes de la signature cryptographique asymétrique pour authentifier les enregistrements. Les signatures et les clés publiques se présentent sous la forme de nouveaux enregistrements complémentaires et permettent d'assurer l'authentification.

Ces nouveaux enregistrements engendrent une augmentation de la taille des messages et du nombre d'échanges pour vérifier les signatures et les clés. DNSSEC nécessite donc plus de ressources machines, ainsi que des versions récentes et à jour de logiciels DNS.

Le protocole a naturellement été conçu pour pouvoir fonctionner sans problème dans un environnement qui, au départ tout au moins, ne sera pas entièrement composé de résolveurs DNSSEC validants. Dans le cas où un résolveur non DNSSEC validant interroge des serveurs DNSSEC, ceux-ci renvoient simplement les informations habituellement échangées sans les signatures ni les enregistrements propres à DNSSEC.

4 Ce que n'est pas DNSSEC

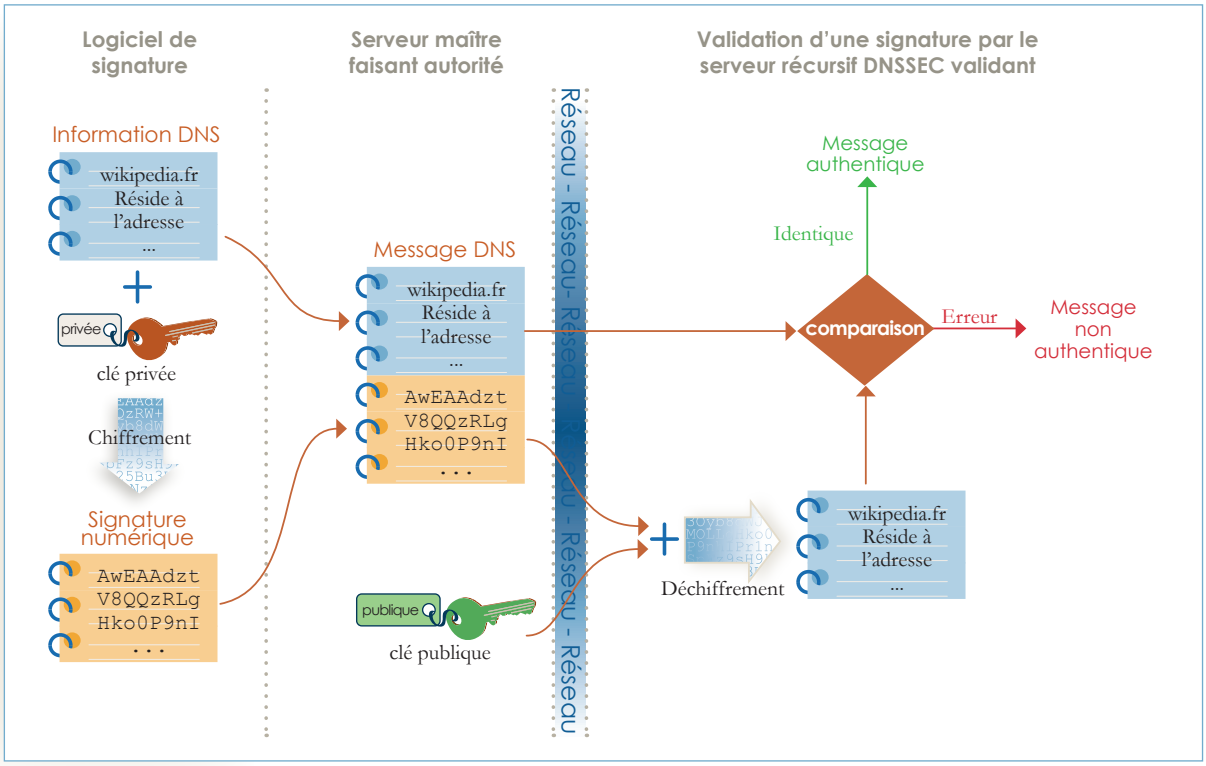
Bien qu'étant à juste titre présenté comme une évolution nécessaire en termes de sécurisation du DNS, DNSSEC ne prétend aucunement répondre à tous les types d'attaques pouvant survenir.

Il n'a, par exemple, pas vocation à crypter les enregistrements DNS, ni à assurer la confidentialité des échanges sur le réseau, ni à garantir la sécurité d'une transaction comme le font les certificats SSL. Il ne protège pas contre le phishing ou le vol de noms de domaine, contre les virus et autres techniques d'infection des postes informatiques, ou encore contre les attaques visant les sites web eux-mêmes (injections SQL…).

De plus, chacun des niveaux de sécurité n'a de sens qu'au sein de la chaîne de confiance : ainsi, des enregistrements signés ne peuvent pas être authentifiés tant que la clé de la zone n'a pas été publiée dans la zone parente. À l'inverse, aucune sécurité particulière n'est apportée à l'utilisateur tant que son résolveur n'a pas mis en oeuvre DNSSEC. Enfin, DNSSEC ne protège pas l'intégrité des données qui auraient été modifiées de manière accidentelle ou volontaire en amont de leur publication dans le DNS.

5 Utilisation des clés dans DNSSEC

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



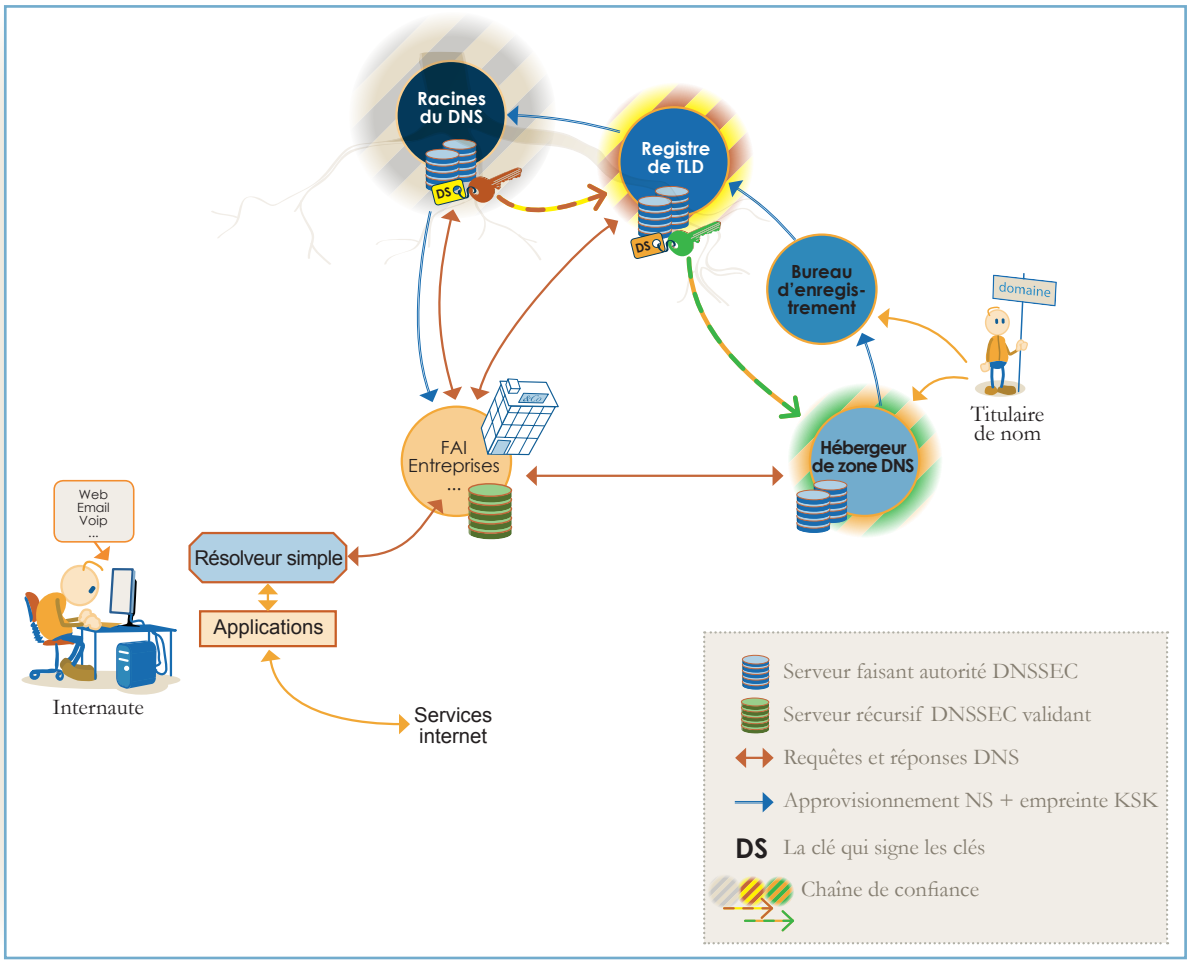
Signature et validation de signature dans le cas du DNS

Un message est chiffré grâce à la clé privée, créant une signature accompagnant le message. Cette signature pourra être authentifiée par les résolveurs DNSSEC validant à l'aide de la clé publique correspondante publiée dans la zone.

Afin d'éviter qu'un attaquant n'utilise son propre jeu de clés, les concepteurs de DNSSEC ont prévu que chaque zone parente, située au niveau supérieur de l'arborescence du DNS, garantisse l'authenticité des clés de ses zones filles en les signant, les échanges de clés entre zones parentes et filles se faisant exclusivement par des canaux sécurisés. Ce système permet de créer de véritables chaînes de confiance jusqu'à la racine du DNS.

DNSSEC nécessite par ailleurs une bonne gestion de la durée de vie des signatures par rapport à la publication des clés, des signatures expirées pouvant conduire au blocage de la résolution pour la zone concernée.

À l'instar des autres enregistrements DNS, les enregistrements DNSSEC ont en effet des durées de vie limitées afin de permettre la résilience du système et d'autoriser des mises à jour en temps utile. Lorsqu'une signature expire, elle est considérée comme invalide et il n'est plus possible de joindre le service. Il est donc nécessaire de resigner régulièrement les enregistrements, en plus des nouvelles signatures produites suite à des créations ou à des modifications d'enregistrements. Le déploiement de DNSSEC induit par conséquent un travail supplémentaire et génère potentiellement de nouveaux risques d'erreurs (mauvaises configurations, expirations de signatures…). Ainsi, si la clé insérée dans la zone parente n'est pas celle qui est utilisée pour signer, la zone fille sera considérée comme invalide et il se produira une erreur de résolution.



Composantes de la chaîne de confiance DNSSEC

6 Le déploiement de DNSSEC

Bien qu'ayant connu une forte montée en puissance depuis la révélation de la Faille Kaminsky, DNSSEC n'est pas une découverte pour les experts du DNS. L'IETF (Internet Engineering Task Force) a en effet commencé à travailler dès 1995 sur un tel protocole de sécurisation du DNS.

Ce n'est pourtant qu'en 2005, après maints travaux au sein de la communauté technique, que le registre de l'extension *.se* (Suède) fut le premier à signer sa zone. C'est aussi lui qui fut le premier à ouvrir ce service aux titulaires de noms de domaine en 2007.

Considéré avec intérêt mais sans caractère d'urgence jusqu'en 2008, DNSSEC devient une priorité forte pour tous les registres d'extensions à partir de l'été 2008, lorsque la Faille Kaminsky révèle à tous de l'ampleur du problème potentiel. Par conséquent, depuis, une quinzaine de registres ont signé leur extension à la mi-2010 et la plupart des autres y travaillent. Le *.fr* pour sa part a été signé le 14 septembre 2010.

S'il passe par les registres, le déploiement de DNSSEC ne s'arrête pas là : les gestionnaires des résolveurs (FAI, bureaux d'enregistrement, entreprises…) doivent à leur tour mettre en place DNSSEC pour que celui-ci fonctionne à plein.

Un certain nombre de solutions existent, depuis les solutions de logiciels libres telles qu'Open-dnssec jusqu'aux boîtiers propriétaires, en passant par les bibliothèques de programmation qui simplifient les développements.

La charge induite par le déploiement de DNSSEC, aussi bien en coûts qu'en termes de mise à niveau des équipes, peut être perçue comme importante en regard des risques qu'il prévient. Bien que potentiellement justifiée à court terme, cette approche ne tient cependant pas compte de l'accroissement du débit des réseaux et des capacités machines, qui fait progresser mécaniquement les chances de succès des attaques par empoisonnement de cache dans le format actuel du fonctionnement du DNS. La mise en oeuvre de DNSSEC doit donc être envisagée comme une nécessité incontournable à moyen terme.

La principale problématique dans le déploiement de DNSSEC est de mettre en place un système efficace de gestion des clés. Celles-ci doivent en effet être régulièrement modifiées afin d'éviter leur vol ou leur recalcul, mais aussi protégées par des dispositifs physiques et numériques. Les mises à jour doivent par ailleurs être opérée de manière à prendre en compte les temps de propagation des informations dans le DNS, afin d'éviter que les résolveurs fassent correspondre une nouvelle signature à une ancienne clé ou l'inverse. Ceci impose des périodes de latence entre la déclaration des clés et la signature avec celles-ci.

La mise en œuvre de DNSSEC implique donc pour chaque zone de :

- Créer des clés.
- Signer ses enregistrements.
- Publier la zone signée.
- Gérer des périodes de validité.
- Gérer les publications du résumé de la clé dans la zone parente avec chaque rotation de KSK.
- Contrôler la publication d'une nouvelle clé avant de l'utiliser pour signer.

7 Quelques questions à se poser au regard de la mise en place de DNSSEC

La mise en oeuvre de DNSSEC n'est pas seulement une évolution technique majeure pour le DNS : elle induit aussi une adaptation de l'organisation de la gestion des noms de domaine et peut conduire à une nécessaire évolution de celle-ci, notamment du fait de l'émergence de nouveaux aspects comme la gestion des clés.

Il convient donc d'anticiper une certaine montée en compétence des équipes techniques – le sujet restant peu connu – mais aussi une évolution des procédures tout en conservant une cohérence globale avec les différents aspects de la politique de sécurité de l'entreprise.

Voici une liste de quelques questions à se poser, sans prétendre à l'exhaustivité :

- Chez qui les zones DNS de l'entreprise sont-elles hébergées ?
- Quelle est la compétence de ce prestataire dans la gestion de DNSSEC ?
- Quel niveau de transparence ce prestataire offre-t-il à ses clients en termes de pratiques ?
- Quels sont les dispositifs de sécurité dont ce prestataire dispose au-delà de DNSSEC ?
- Ce prestataire offre-t-il des canaux de transactions sécurisés ?
- Quel mode d'organisation ce prestataire préconise-t-il pour la gestion des clés, au sein de son équipe et en articulation avec celles de l'entreprise ?
- Y a-t-il une incidence en termes de coûts à la mise en place de DNSSEC ?
- Si l'entreprise passe par un prestataire pour la signature de ses zones, comment gérer un transfert à un autre prestataire de ses noms de domaine signés ?
- Le niveau de dépendance induit à l'égard de ce prestataire est-il acceptable, ou de nature à inciter l'entreprise à internaliser cette fonction au moins pour ses noms de domaine les plus stratégiques ?
- Si oui, quelles sont les ressources et les capacités dont dispose l'entreprise sur ces problématiques et quels moyens seraient-ils nécessaires pour accompagner une éventuelle montée en puissance ?

8 Pour aller plus loin

- Espace DNSSEC du site de l'AFNIC : www.afnic.fr/dnssec
- Page DNSSEC de Wikipedia en français : http://fr.wikipedia.org/wiki/DNSSEC

Pour toute information supplémentaire sur les actions de l'AFNIC relatives à DNSSEC :

solutions@afnic.fr

9 Glossaire

DNS :
Domain Name System. Service distribué permettant d'enregistrer les ressources de l'Internet (adresse de serveurs, de routeurs, ...) sous la forme d'un nom de domaine.

DNSKEY :
Enregistrement DNS servant à stocker la partie publique d'une clé.

DNSSEC :
Domain Name System Security Extensions. Ensemble d'extensions de sécurité du protocole DNS.

DS :
Delegation Signer. Enregistrement DNS qui correspond à l'empreinte de la partie publique d'une clé.

KSK :
Key Signing Key. Clé qui signe les clés ZSK. L'empreinte de sa partie publique est publiée dans la zone parente pour créer une chaîne de confiance garantissant son authenticité ainsi que l'authenticité des clés signant la zone.

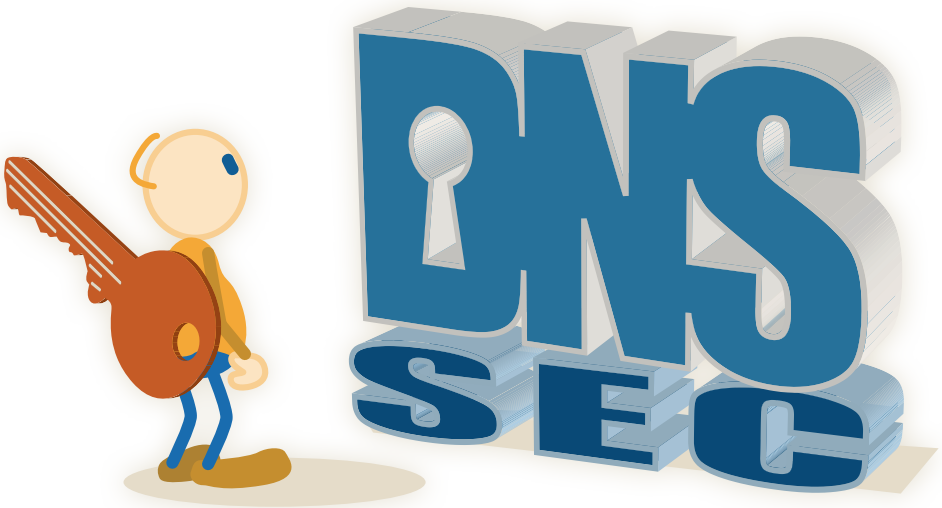
NS :
Name Server. Appelé aussi serveur DNS ou serveur de nom. Serveur utilisé pour héberger un nom de domaine.

SSL :
Secure Sockets Layer. Protocole de sécurisation des échanges sur Internet.

SQL :
Structured Query Language. Langage informatique normalisé qui sert à demander des opérations sur des bases de données.

ZSK :
Zone Signing Key. Clé qui signe les enregistrements de la zone. La partie publique de la ZSK permet de vérifier les signatures.

Retrouvez tous les dossiers thématiques de l'AFNIC :
www.afnic.fr/actu/presse/liens-utiles



web **www.afnic.fr - afnic@afnic.fr**