DNSSEC

Pour la sécurité sur Internet

SWITCH
Serving Swiss Universities

Que signifie DNSSEC?

DNSSEC est une extension du système de noms de domaine (DNS) servant à garantir l'authenticité et l'intégrité des données de réponses DNS.

Par des mesures techniques, l'ordinateur demandeur (par exemple navigateur Internet) peut ainsi reconnaître si la réponse sur une adresse Internet au DNS provient effectivement du serveur enregistré chez nous comme compétent. En même temps, il est garanti que cette réponse n'a pas été modifiée pendant le transport sur Internet.

Plus simplement: DNSSEC est une sorte d'assurance garantissant à l'usager d'Internet que seul est affiché le site Web qu'il souhaite appeler.

Ceci est garanti par des signatures cryptographiques. Les informations ne sont pas codées sur DNSSEC. Toutes les données restent publiquement accessibles comme pour le DNS existant.

Pourquoi a-t-on besoin de DNSSEC?

Le lecteur attentif a certainement remarqué qu'une technologie destinée à garantir à l'usager le site Web «correct» est déjà intégrée au navigateur Internet. De tels sites sont généralement codés par SSL (Secure Sockets Layer) et marqués au navigateur d'un symbole de clé.

DNSSEC n'a pas été développé pour remplacer le codage SSL. Au contraire, il doit compléter SSL et empêcher que l'on arrive au mauvais serveur avant même que la liaison par SSL ait été assurée.

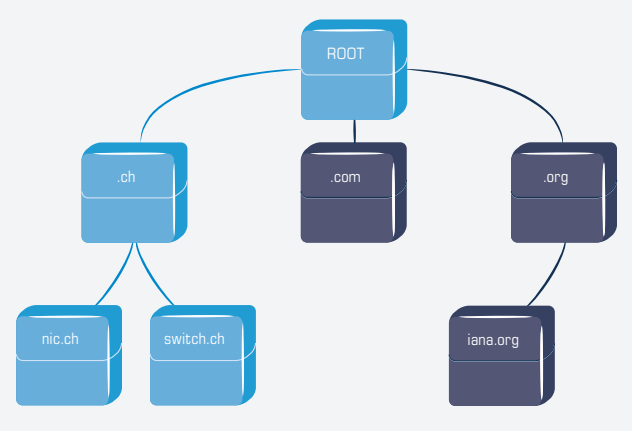
Comment le DNS (Domain Name System) fonctionne-t-il?

Internet, tel que nous le connaissons actuellement, est basé sur le système mondial de noms de domaine. Nous aimerions en expliquer rapidement le fonctionnement.

On peut se représenter le DNS comme une sorte d'annuaire téléphonique réparti sur le monde affectant les noms de domaine univoques au niveau mondial (www.switch.ch) aux adresses Internet elles aussi mondialement univoques (130.59.138.34). Les adresses Internet ou noms de domaine servent uniquement à simplifier l'écriture.

Afin que toutes les demandes n'aboutissent pas à un seul serveur, le DNS est de structure hiérarchique. L'espace de nom est partagé en se qu'on appelle des zones. Pour www.switch.ch, cela serait selon le plus haut niveau hiérarchique (Root) les serveurs pour la Suisse («ch») puis les serveurs de SWITCH («switch.ch»). Les compétences des zones sont partagées (déléguées) dans la hiérarchie.

Lorsque vous voulez appeler avec votre ordinateur le site www.switch.ch, le serveur de noms de votre fournisseur d'accès Internet interrogera l'un après l'autre tous les niveaux de la hiérarchie. Chaque niveau ne connaissant pas la réponse sur l'adresse cible renverra au niveau immédiatement inférieur. Le serveur le plus bas de la hiérarchie pourra finalement donner la réponse à l'adresse.



Le Domain Name System (DNS) est de structure hiérarchique. Les serveurs de noms pour «.ch» transmettent les demandes de noms de domaine se terminant par .ch (par ex. switch.ch) automatiquement à l'adresse correcte.

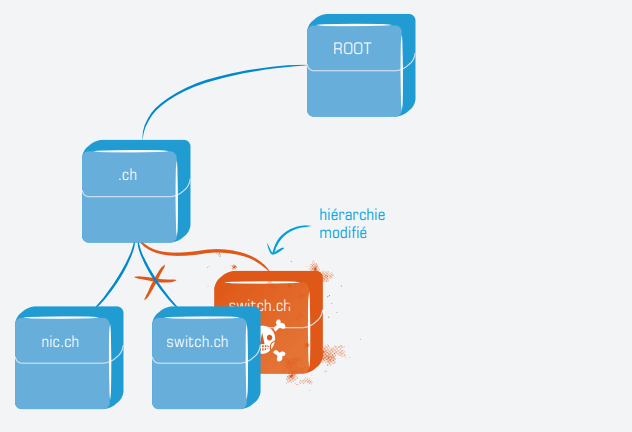
A quoi sert DNSSEC?

Imaginez que quelqu'un parvienne à modifier des inscriptions à l'annuaire téléphonique. Vous chercher le numéro du Help Desk SWITCH et trouvez un faux numéro. Auriez-vous la possibilité de détecter l'abus? Certainement pas.

Sur Internet, un tel scénario est possible si un attaquant modifie la hiérarchie des sites ci-dessus. S'il parvenait par exemple à introduire des données erronées au serveur de votre fournisseur (cache poisoning), en appelant www.switch.ch, vous tomberiez sur un autre site Web. Mieux vaut ne pas songer à ce qui pourrait se passer si le site falsifié était celui de votre banque. Ou si vous envoyiez la dernière stratégie de votre société au serveur mail d'un partenaire.

Etant donné qu'Internet est utilisé actuellement à toutes les fins possibles et imaginables, de telles attaques de pirates peuvent avoir de graves conséquences. DNSSEC offre une protection de base de telles attaques – et non seulement à l'appel de sites.

Le «Cache-Poisoning» permet de modifier la hiérarchie.



DNSSEC ne peut pas protéger d'une manière générale des attaques de Phishing mais offre une protection efficace contre les attaques au DNS. Ceci est important car la plupart des attaques de Phishing peuvent être décelées et empêchées par des usagers vigilants d'Internet. Cependant, les attaques au DNS ne sont guère décelables même par des experts.

DNSSEC en détail

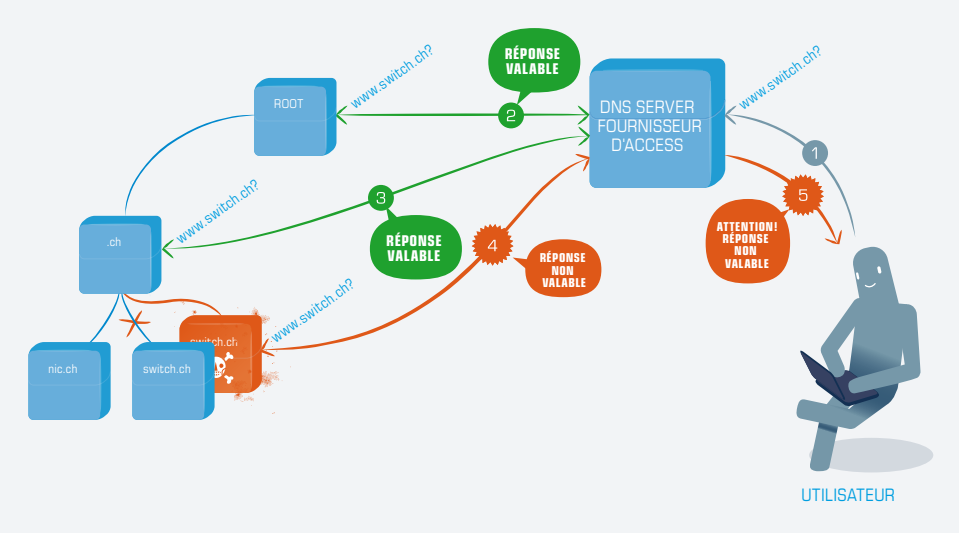
Comme déjà mentionné, DNSSEC est basé sur les signatures cryptographiques permettant de signer les inscriptions DNS actuelles.

Toute personne compétente ayant autorité pour un nom de domaine sur Internet peut protéger ses informations par DNSSEC.

Toutes les informations pour lesquelles un fournisseur de services est compétent sont signées de son code privé et les signatures sont inscrites au DNS (RRSIG Record).

Un exemple avec DNSSEC:
Le serveur de noms de votre fournisseur Internet suit à nouveau la hiérarchie connue pour résoudre une question. Cette fois-ci, il peut cependant vérifier, sur la base des signatures reçues, si l'origine des réponses est juste et si une réponse a été modifiée en route. Il ne répondra qu'une fois que toutes les informations seront correctes.

Avec DNSSEC, le serveur de noms de votre fournisseur d'accès Internet peut identifier une hiérarchie modifiée par «Cache-Poisoning».

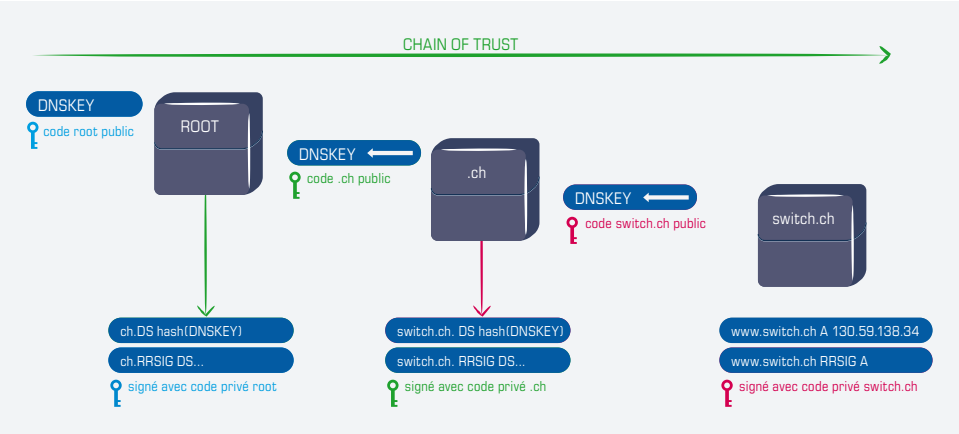


Mais comment toutes ces signatures peuvent-elles être vérifiées?

Pour établir des signatures numériques, il est généré une paire de codes. Une telle paire de codes se compose d'un code privé et d'un code public (système cryptographique asymétrique). Comme le nom le dit, la partie privée est secrète et reste chez le propriétaire. La partie publique est publiée au DNS (DNSKEY Record). Le code public permet de vérifier et de valider une signature qui a été donnée avec le code privé.

On doit donc faire confiance à un code public avant de pouvoir vérifier une signature. Etant donné qu'il n'est pas possible de faire confiance à tous les codes sur Internet, il est utilisé une hiérarchie des codes analogue à la hiérarchie DNS («chain of trust»). Cela paraît un peu embrouillé à première vue mais sert uniquement à pouvoir vérifier toutes les signatures avec un seul code public.

Dans une «Chain of trust», l'instance supérieure garantit (par ex. un serveur de noms pour .ch) l'authenticité des données de l'instance inférieure.



«Chain of trust» en détail

Une image du code public est toujours communiquée au niveau suivant de la hiérarchie. L'instance supérieure inscrit cette image à sa zone (DS Record) et garantit l'authenticité par signature. Le code public de cette instance est à son tour communiqué à l'instance immédiatement supérieure.

De quoi ai-je besoin pour utiliser DNSSEC?

En tant qu'usager d'Internet, on n'a rien à entreprendre. Si votre fournisseur ADSL ou de modem à câble supporte DNSSEC, toutes les signatures sont vérifiées sur ses serveurs DNS.

En tant que détenteur d'un nom de domaine, votre gestionnaire compétent de site doit installer DNSSEC pour vous. Etant donné que DNSSEC ne sera pas encore très répandu dans un premier temps, il est probable que seuls des gestionnaires de sites devant être protégés (banques par exemple) protégeront leurs noms de domaine avec DNSSEC.

SWITCH
Werdstrasse 2
Case postale
CH-8021 Zurich

Téléphone +41 848 844 080
Fax +41 848 844 081
helpdesk@nic.ch
www.nic.ch/fr/dnssec