DNSSEC

Für ein sicheres Internet

SWITCH
Serving Swiss Universities

Was ist DNSSEC?

DNSSEC ist eine Erweiterung des Domain Namen Systems (DNS), die dazu dient, die Echtheit (Authentizität) und die Vollständigkeit (Integrität) der Daten von DNS-Antworten sicherzustellen.

Durch technische Massnahmen kann der anfragende Computer (z.B. Internet Browser) somit erkennen, ob die Antwort nach einer Internet-Adresse im DNS tatsächlich von jenem Server kommt, der bei uns als zuständig eingetragen ist. Gleichzeitig wird sichergestellt, dass diese Antwort auf dem Transport über das Internet nicht verändert wurde.

Vereinfacht gesagt: DNSSEC ist eine Art Versicherung, die dem Internetnutzenden garantiert, dass nur diejenige Webseite angezeigt wird, die er aufrufen will.

Diese Garantie wird mittels kryptografischer Unterschriften gewährleistet. Bei DNSSEC werden keine Informationen verschlüsselt. Alle Daten bleiben wie beim bestehenden DNS öffentlich zugänglich.

Wieso braucht man DNSSEC?

Der aufmerksame Leser hat sicherlich erkannt, dass im Internet Browser schon eine Technologie integriert ist, welche dem User die «richtige» Webseite garantieren soll. Solche Webseiten sind meist mit SSL (Secure Sockets Layer) verschlüsselt und werden im Browser mit einem Schlüsselsymbol gekennzeichnet.

DNSSEC wurde nicht entworfen, um die SSL-Verschlüsselung abzulösen. Im Gegenteil, DNSSEC soll SSL ergänzen und verhindern, dass man nicht schon auf einem falschen Server landet, bevor die Verbindung durch SSL gesichert wurde.

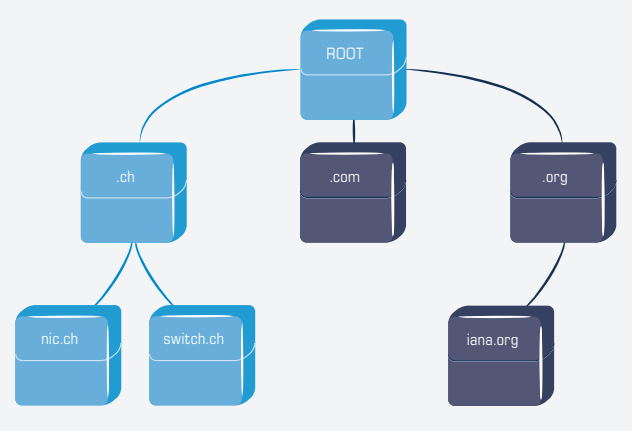
Wie funktioniert das DNS (Domain Name System)?

Das Internet wie wir es heute kennen basiert auf dem globalen Domain Name System. Dessen Funktionsweise möchten wir im Folgenden kurz erklären.

Das DNS kann man sich als global verteiltes Telefonbuch vorstellen, das die weltweit eindeutigen Domain-Namen (www.switch.ch) den weltweit eindeutigen Internet-Adressen (130.59.138.34) zuordnet. Die Internet-Adressen oder auch Domain-Namen dienen nur der vereinfachten Schreibweise.

Damit nicht alle Anfragen auf einem einzigen Server landen, ist das DNS hierarchisch aufgebaut. Der Namensraum wird in so genannte Zonen aufgeteilt. Für www.switch.ch wären das nach der obersten Hierarchie (Root) die Server für die Schweiz («ch») und dann die Server von SWITCH («switch.ch»). Die Zuständigkeiten der Zonen werden in der Hierarchie aufgeteilt (delegiert).

Wenn Sie mit Ihrem Rechner die Webseite www.switch.ch aufrufen wollen, wird der Nameserver Ihres Internetanbieters alle Stufen der obigen Hierarchie nacheinander abfragen. Jede Stufe, die die Antwort nach der Ziel-Adresse nicht kennt, gibt einen Hinweis auf die nächsttiefere Stufe. Der Server zuunterst in der Hierarchie kann am Schluss die Antwort nach der Adresse beantworten.



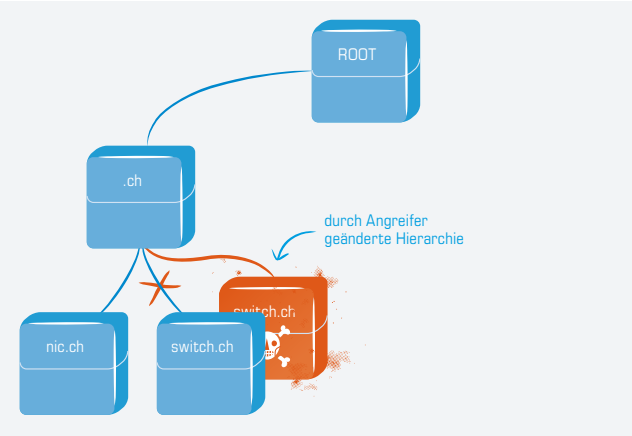
Das Domain Name System (DNS) ist hierarchisch aufgebaut. Die Nameserver für «.ch» leiten Anfragen für Domain-Namen mit der Endung .ch (z.B. switch.ch) automatisch an die richtige Adresse weiter.

Was nützt DNSSEC?

Stellen Sie sich vor, jemandem gelingt es, Einträge im Telefonbuch zu ändern. Sie schlagen also die Nummer des SWITCH-Helpdesks nach und finden eine falsche Nummer. Hätten Sie eine Möglichkeit, unerlaubten Missbrauch zu erkennen? Wohl kaum.

Im Internet ist solch ein Szenario möglich, indem ein Angreifer die oben beschriebene Hierarchie ändert. Falls es einem Angreifer gelingt, zum Beispiel falsche Daten in den Server Ihres Providers einzuschleusen (Cache Poisoning), würden Sie beim Aufruf von www.switch.ch auf einer anderen Webseite landen. Stellen Sie sich besser nicht vor, was passieren könnte, wenn es sich bei der gefälschte Webseite um die Ihrer Bank handelt. Oder wenn Sie die neueste Strategie Ihrer Firma dem «falschen» Mailserver eines Partners senden.

Durch «Cache-Poisoning» kann die Hierarchie verändert werden.



Da das Internet heute für alle möglichen Zwecke verwendet wird, können solche Hackerangriffe weitgreifende Auswirkungen haben. DNSSEC bietet einen grundlegenden Schutz vor solchen Attacken – nicht nur beim Aufruf von Webseiten.

DNSSEC kann nicht generell vor Phishing-Attacken schützen. Es bietet aber einen wirksamen Schutz vor Angriffen auf das DNS. Dies ist wichtig, da die meisten Phishing- Attacken von wachsamen Internetnutzenden entdeckt und verhindert werden können. Angriffe auf das DNS sind jedoch selbst für Experten kaum zu erkennen.

DNSSEC im Detail

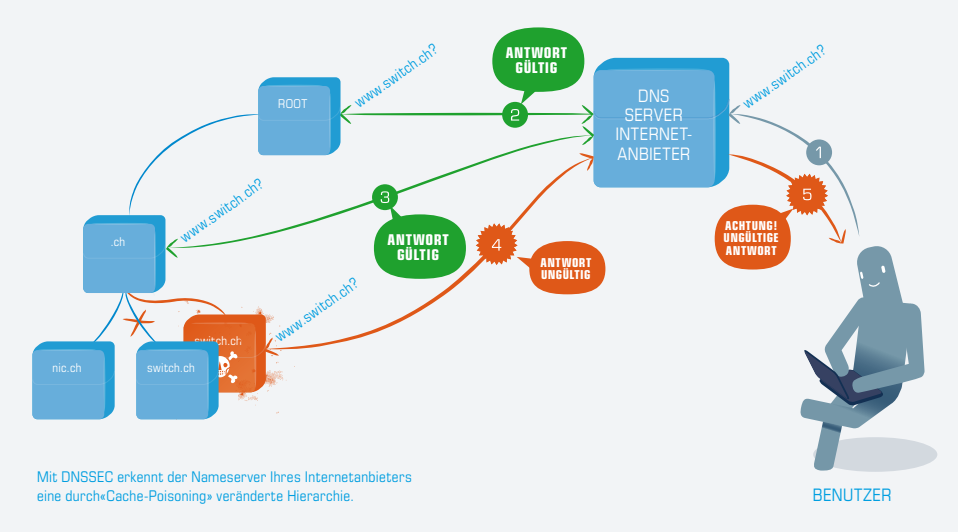
Wie erwähnt, basiert DNSSEC auf kryptografischen Unterschriften oder Signaturen, mit denen die aktuellen DNS-Einträge unterschrieben (signiert) werden. Jeder, der im Internet für einen Domain-Namen (autoritativ) zuständig ist, kann seine Informationen mittels DNSSEC schützen.

Alle Informationen, für die ein Dienstanbieter zuständig ist, werden mit dessen privatem Schlüssel unterschrieben und die Signaturen werden ins DNS geschrieben (RRSIG Record).

Ein Beispiel mit DNSSEC

Der Nameserver Ihres Internetanbieters folgt zur Auflösung einer Frage wieder der bekannten Hierarchie. Dieses Mal kann er jedoch anhand der empfangenen Unterschriften prüfen, ob die Herkunft der Antworten stimmt und ob eine Antwort unterwegs verändert wurde. Erst wenn alle Informationen korrekt sind, wird er antworten.

Mit DNSSEC erkennt der Nameserver Ihres Internetanbieters eine durch «Cache-Poisoning» veränderte Hierarchie.



Mit DNSSEC erkennt der Nameserver Ihres Internetanbieters eine durch«Cache-Poisoning» veränderte Hierarchie.

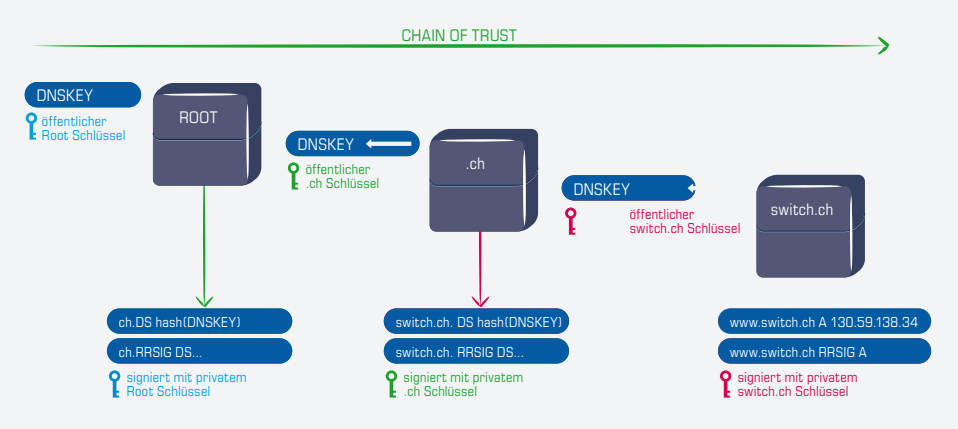
Wie können nun aber alle diese Unterschriften überprüft werden?

Um digitale Signaturen zu erstellen, wird ein Schlüsselpaar generiert. Ein solches Schlüsselpaar besteht aus einem privaten und einem öffentlichen Schlüsselpaar (asymmetrisches Kryptosystem). Wie der Name schon sagt, ist der private Teil geheim und verbleibt beim Besitzer. Der öffentliche Teil wird im DNS publiziert (DNSKEY Record). Mit dem öffentlichen Schlüssel kann nun eine Unterschrift, welche mit dem privaten Schlüssel signiert wurde, überprüft und validiert werden.

Einem öffentlichen Schlüssel muss man also vertrauen, bevor man eine Unterschrift überprüfen kann. Da es nicht möglich ist, allen Schlüsseln im Internet zu vertrauen, wird eine Schlüsselhierarchie analog der DNS Hierarchie verwendet («chain of trust»). Das sieht auf den ersten Blick etwas verwirrend aus. Es dient aber nur dazu, alle Unterschriften mit einem einzigen öffentlichen Schlüssel überprüfen zu können.

«Chain of trust» im Detail

In einer «Chain of trust» garantiert die übergeordnete Instanz (z.B. der Nameserver für .ch) die Echtheit von Daten der untergeordneten Instanz.



Ein Abbild des öffentlichen Schlüssels wird jeweils der nächsten Stufe in der Hierarchie mitgeteilt. Die höhere Instanz schreibt dieses Abbild in ihre Zone (DS Record) und garantiert für die Echtheit durch Signieren. Der öffentliche Schlüssel dieser Instanz wird wiederum der nächsthöheren Instanz übermittelt.

Was brauche ich, um DNSSEC zu nutzen?

Als Internetnutzer muss man nichts unternehmen. Wenn Ihr ADSL oder Kabelmodem-Anbieter DNSSEC unterstützt, erfolgen alle Überprüfungen der Unterschriften auf dessen DNS-Servern.

Als Inhaber eines Domain-Namens muss Ihr zuständiger Webseiten-Betreiber DNSSEC für Sie einrichten. Da DNSSEC gerade in der Anfangsphase noch nicht weit verbreitet sein wird, werden vermutlich zu Beginn erst Betreiber schützenswerter Webseiten (z.B. Banken) ihre Domain-Namen mit DNSSEC schützen.

SWITCH
Werdstrasse 2
Postfach
CH-8021 Zürich

Telefon +41 848 844 080
Fax +41 848 844 081
helpdesk@nic.ch
www.nic.ch/de/dnssec