PRESSEMITTEILUNG

DENIC führt DNSSEC für die deutsche Top Level Domain .de ein

Am 31. Mai 2011 hat die deutsche Registrierungsstelle DENIC den letzten Schritt zur Einführung von DNSSEC für .de vollzogen: die .de-Zone ist mit dem endgültigen, zur Validierung einsetzbaren öffentlichen Schlüssel bestückt worden.

Zudem hat DENIC den so genannten DS-Record, der auf diesen öffentlichen Schlüssel für .de verweist und Voraussetzung für die Validierung von DNSSEC-signierten Domains ist, bei der Internet Assigned Numbers Authority (IANA) für eine Veröffentlichung in der Rootzone eingereicht. Dieser DS-Record wird voraussichtlich bis Mitte Juni in der Rootzone erscheinen und ab dann die weltweite Validierung signierter .de-Domains ermöglichen.

Die Signierung einer Domain kann über den Web- oder Domaindienstanbieter erfolgen oder durch den Domaininhaber selbst. Im Falle der Signierung durch den Anbieter – Voraussetzung ist, er unterstützt DNSSEC – ist dieser für die Schlüsselerzeugung, Signierung der Zonendaten, Neusignierung vor Ablauf der Signaturgültigkeit sowie den regelmäßig notwendigen Schlüsselwechsel zuständig. Domaininhaber, die ihre Domain mit DNSSEC schützen möchten, können dies ab sofort tun und wenden sich dazu bitte an ihren Provider, der auch die Registrierung der Schlüssel bei DENIC übernimmt.

Um als Internetnutzer die Vorteile von DNSSEC zu nutzen, benötigen Sie einen validierenden Resolver, der die durch DNSSEC gelieferte Zusatzinformation auswerten kann. Sofern Sie selbst keinen validierenden Resolver betreiben, wird dies in der Regel Ihr Internet Service Provider (ISP) übernehmen. Beim Aufruf von Webseiten leitet das auf dem Rechner installierte Betriebssystem automatisch die DNS-Anfragen an die vom jeweiligen ISP festgelegten DNS-Server. Dort kann die Überprüfung der signierten DNS-Daten auf Echtheit stattfinden.

Für Betreiber validierender Resolver ist die Konfiguration eines Trust-Anchors für .de – neben dem für die Rootzone – nicht notwendig und auch nicht empfehlenswert, da mit einer solchen Konfiguration etwaige spätere Schlüsselwechsel unbemerkt bleiben könnten, was Validierungsfehler und Ausfälle zur Folge hätte.

Weitere Informationen zum Thema DNSSEC finden Sie auf unserer Webseite unter http://www.denic.de/dnssec.

Hintergrundinformationen zu DNSSEC

Domain Name System Security Extensions (DNSSEC) sind eine Erweiterung des DNS (Domain Name System), die darauf abzielt, Sicherheitslücken im Internet – wie Cache-Poisoning und DNS-Spoofing – zu schließen.

DNSSEC bietet Sicherheit durch Quellenauthentisierung, das heißt, durch die Sicherung des Pfades zwischen DNS-Servern und validierenden DNS-Klienten, wobei auch dazwischen liegende Resolver mit ihren Caches mit in die Sicherheitskette eingeschlossen sind. Anhand der verwendeten Signatur lässt sich prüfen, ob die Daten von einer dazu berechtigten Stelle erzeugt wurden. Gleichzeitig bietet die Integritätssicherung Schutz vor Verfälschungen der DNS-Daten auf dem Transportweg. DNSSEC kann jedoch keine Aussagen bezüglich der Korrektheit der initial eingestellten Daten liefern. Auch Domain-Hijacking oder Eingriffe in Registrierungsprozesse lassen sich damit nicht feststellen.

DNSSEC prüft DNS-Antworten anhand von kryptografisch gesicherten Signaturen, die über die zu schützenden DNS-Inhalte errechnet und zusammen mit diesen an den Client übertragen werden. Die Prüfung der Antworten und Signaturen erfolgt im Client oder in dem davor liegenden Resolver gegenüber den zur jeweiligen Zone passenden öffentlichen Schlüsseln. Diese Schlüssel können ebenfalls am einfachsten wiederum im DNS hinterlegt und abgerufen werden. Dabei ist kein Bruch des Sicherheitsmechanismus möglich, da auch der Transfer der Schlüssel mit Hilfe von DNSSEC abgesichert erfolgt und lediglich der für den Beginn der Kette notwendige Schlüssel (der Key der Rootzone) im Client fest hinterlegt oder per Konfiguration eingepflegt wird.

DNSSEC ist ein Baustein, um den Betrieb des DNS – ein zentraler Aspekt des Internets – sicherer zu machen, indem es vor Fälschungen und dem Unterschieben falscher DNS-Daten schützt.

Die DENIC eG

Als zentrale Registrierungsstelle verwaltet DENIC inzwischen mehr als 14 Millionen Domains unterhalb der Top Level Domain .de und stellt damit eine wesentliche Ressource für die Nutzer des Internets bereit. Mit der Mission, als neutraler und kompetenter Dienstleister für alle Domaininhaber und Internetnutzer zu agieren, legen die mehr als 120 Mitarbeiter den Grundstein dafür, dass deutsche Internetseiten und E-Mail-Adressen weltweit erreichbar sind. Die über 270 Mitglieder der Genossenschaft sind deutsche wie internationale Unternehmen aus dem IT- und TK-Bereich. Gemeinsam mit ihnen und anderen Kooperationspartnern setzt sich DENIC für den sicheren Betrieb und die weltweite Weiterentwicklung des Internets ein. Dabei arbeitet DENIC ohne Gewinnerzielungsabsicht.

Zu den Aufgaben von DENIC gehören der Betrieb des automatischen elektronischen Registrierungssystems für die Mitglieder, der Betrieb der Domain-Datenbank für die Top Level Domain .de und die deutsche ENUM-Domain (.9.4.e164.arpa), der Betrieb des Nameserverdienstes für die .de-Zone und die deutsche ENUM-Domain an derzeit 16 Standorten auf der ganzen Welt sowie die Mitgestaltung der organisatorischen und technischen Weiterentwicklung des Internets in Zusammenarbeit mit internationalen Gremien (z. B. ICANN, CENTR, IETF).

Bei Fragen wenden Sie sich bitte an:

DENIC eG
Pressereferat
Fon: +49 69 27235-274
Email: presse@denic.de

DENIC eG
Kaiserstraße 75 - 77
60329 Frankfurt am Main
GERMANY

Email: presse@denic.de
Fon: +49 69 27235-274
Fax: +49 69 27235-235
http://www.denic.de

Angaben nach § 25a Absatz 1 GenG:
DENIC eG (Sitz: Frankfurt am Main)
Vorstand: Sabine Dolderer, Helga Krüger, Carsten Schiefner, Dr. Jörg Schweiger
Vorsitzender des Aufsichtsrats: Elmar Knipp
Eingetragen unter Nr. 770 im Genossenschaftsregister, Amtsgericht Frankfurt am Main