



## Press Release

### DENIC Launching DNSSEC for the German Top Level Domain .de

On 31 May 2011, the German registry DENIC took the last step required to launch DNSSEC for .de: The .de zone now contains the final public key, which is suited for validation.

Moreover, DENIC has submitted to the Internet Assigned Numbers Authority (IANA) the so-called DS record for publication in the root zone. The DS record refers to the public key for .de and is a mandatory prerequisite for validating DNSSEC-signed domains. It will probably become visible in the root zone by mid-June and from then on allow validation of signed .de domains all across the Internet.

Signing of a domain can be carried out either through the web or domain service provider or by the domain holders themselves. If signing is performed by one of these service providers – which may be an optional service – this provider also is responsible for generating the keys, signing the zone data, carrying out re-signing before signatures expire, and for changing the keys at the required intervals. Domain holders who want to protect their domains with DNSSEC can do this from now on. They are kindly requested to contact their registrar, who will also register the keys with DENIC.

To be able to benefit from DNSSEC as an Internet user you need a validating resolver that is capable to interpret the additional information supplied by DNSSEC. If you do not operate a validating resolver yourself, your Internet service provider (ISP) will normally operate such a resolver for you. When you visit a website, the operating system installed on the computer automatically directs the DNS query to the DNS server defined by the respective ISP. That server will validate data authenticity.

Operators of validating resolvers do not need to configure a trust anchor for .de in addition to the one used for the root zone. It is not recommended either, since such a configuration might lead to later key rollovers not being noticed. This, in turn, might entail validation errors and failures.

You will find detailed information about DNSSEC on our website at <http://www.denic.de/en/domains/dnssec.html>.

## About DNSSEC

Domain Name System Security Extensions (DNSSEC) are extensions of the DNS (Domain Name System) which have the purpose to close security holes in the Internet, such as cache poisoning and DNS spoofing.

DNSSEC provides security by data origin authentication, i.e. by securing the path between the DNS servers and the validating DNS clients, with intermediate resolvers and their caches being included in the security perimeter. The signature which was applied reveals if the data were actually generated by a source entitled to do so. At the same time, securing data integrity protects against DNS data that was manipulated on the way. However, DNSSEC does not warrant the correctness of the initially stored data. Neither will it protect against domain hijacking or manipulations during the registration process.

DNSSEC verifies DNS replies by means of cryptographically secured signatures. These signatures are computed from the DNS data to be protected and are transferred to the client together with the data. Response verification is executed in the client or in the upstream resolver by means of a check against the public keys valid for the respective zone. These keys, in turn, are easily stored in and retrieved from the DNS. This procedure itself is secured by DNSSEC and is thus not subject to the aforementioned security threats; only the key required to start the chain of trust (i.e. the key of the root zone) is permanently stored in the client or its configuration data.

DNSSEC is one component to make operation of the DNS – a crucial aspect of the Internet – more secure by protecting the DNS against data manipulation and spoofing.

## About DENIC

As the central registry, DENIC administers the now more than 14 million domains under the Top Level Domain .de and thus provides a crucial resource for users of the Internet. It sees its role as that of a competent, impartial provider of services for all domain holders and Internet users. With more than 120 employees, DENIC creates the foundation through its work for German Internet pages and e-mail addresses to be accessible throughout the world. The about 270 members of the Cooperative are IT or telecommunications businesses based in Germany and elsewhere. Working in cooperation with them and other partners, DENIC is committed to guarantee the secure operation of the Internet and its further worldwide development as a not-for-profit organization.

It operates the automatic electronic registration system for its members, runs the domain database for the Top Level Domain .de and the German ENUM domain (.9.4.e164.arpa), manages the name server services for the .de zone at currently 16 locations distributed throughout the world, and renders a considerable contribution to the further organizational and technical development of the Internet in cooperation with international bodies (e.g. ICANN, CENTR, IETF).

If you have any questions, please contact:

DENIC eG  
Public Relations  
Fon: +49 69 27235-274  
Email: [presse@denic.de](mailto:presse@denic.de)

-----  
DENIC eG  
Kaiserstraße 75 - 77  
60329 Frankfurt am Main  
GERMANY

e-mail: [presse@denic.de](mailto: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