**What is it?**

DNSSEC is a protocol that is currently being deployed to secure the Domain Name System (DNS), the Internet’s global phone book. Humans prefer locating Internet resources using names (such as www.icann.org), but behind the scenes, DNS converts each name to a numeric address so that data transfers to the right device.

DNSSEC abbreviates “DNS Security Extensions.” DNSSEC adds security to the DNS by incorporating public key cryptography into the DNS hierarchy, resulting in a single, open, global Public Key Infrastructure (PKI) for domain names. It is the result of over a decade of community based, open standards development in the IETF and elsewhere.

**What are DNSSEC benefits?**

A lookup secured with DNSSEC is digitally signed, protecting it against surreptitious modification and therefore against attacks that may, for example, redirect an end user to an imposter or malicious site for password collection. When carried out via an attack on a corporation’s or an ISP’s infrastructure, all of the entity’s users are affected. This is often referred to as cache poisoning. Protection against cache poisoning is one of DNSSEC’s primary benefits.

However, one of the greatest benefits is likely to arise from nascent efforts to use this newly created global PKI to secure more than just domain names. By using DNSSEC to also distribute records (keys) to help secure email, web sites, identities, communications, configurations, and programs, companies and consumers may soon be able to expect seamless, trustworthy communication across organizational and national borders. Signing the root and Top-Level Domains has opened the door for this.

**How do I implement DNSSEC?**

**For Companies:**
- Deploy DNSSEC on your domain names (“sign” your corporate domain names or ask your Registrar for DNSSEC)
- Deploy DNSSEC on corporate DNS infrastructure (turn DNSSEC validation “on” on your corporate DNS resolvers)

**For Users:**
- Ask your ISP about DNSSEC (DNSSEC support on their DNS resolvers)

**ICANN’s Role**

- Manage the root key of this hierarchy together with partners VeriSign, NTIA and trusted international representatives of the Internet community.
- Process requests for additions/changes/deletions of public key and other records from Registries at the top of the DNS hierarchy (i.e., .com, .se, ...etc)
- Educate and assist the Internet community regarding DNSSEC

---

[Diagram showing the difference between DNSSEC and non-DNSSEC scenarios]
**DNSSEC** Securing the Internet

**For Technical Advice:**

- **IETF**
  - [http://www.ietf.org](http://www.ietf.org)

- **ISOC Deploy360 Programme**

- **DNSSEC Deployment Initiative**
  - [http://www.dnssec-deployment.org](http://www.dnssec-deployment.org)

- **ISC**
  - [http://www.isc.org](http://www.isc.org)

- **NLNETLABS**
  - [http://www.nlnetlabs.nl](http://www.nlnetlabs.nl)

- **DNSSEC.NET**
  - [http://www.dnssec.net](http://www.dnssec.net)

- **ICANN**

**Status (2 April 2012):**

- Deployed on 85/313 TLDs (.uk, .fr, .asia, .in, .lk, .tm, .am, .tw, .jp, .cr, .com, .org, .. etc)
- Root signed 2010
- 84% of domain names could have DNSSEC deployed on them
- Large ISPs have begun supporting DNSSEC or committed to do so
- Standards for new applications using DNSSEC are being developed
- But deployed on < 1% of 2nd level domains. Many have plans. Few have taken the step (e.g., paypal.com)
- Need to increase awareness for domain name holders

---