

# DNSSEC

Document available online at:  
<http://dnssec-deployment.icann.org/dnsseccard.pdf>



## 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 servers using names (such as [icann.org](http://icann.org)), but behind the scenes, DNS matches 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.

## 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, 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 set the stage for this.

## How do I implement DNSSEC?

### For Companies:

Deploy DNSSEC on corporate DNS infrastructure (turn DNSSEC validation "on")

Deploy DNSSEC on your domain names ("sign" your corporate domain names)

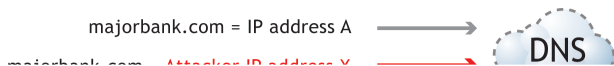
### For Users:

Ask your ISP about DNSSEC (get DNSSEC validation turned "on" on their DNS servers)

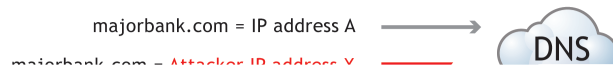
## ICANN's Role

- Manage the root key of this hierarchy together with VeriSign (under contract with the US Department of Commerce) 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

### Without DNSSEC



### With DNSSEC



## For Technical Advice:

- |                                |   |
|--------------------------------|---|
| • IETF                         | <a href="http://www.ietf.org">http://www.ietf.org</a> , <a href="http://tools.ietf.org/pdf/draft-ietf-dns-ops/rfc4641bis-05.pdf">http://tools.ietf.org/pdf/draft-ietf-dns-ops/rfc4641bis-05.pdf</a> |
| • DNSSEC Deployment Initiative | <a href="http://www.dnssec-deployment.org">http://www.dnssec-deployment.org</a>   |
| • ISC                          | <a href="http://www.isc.org">http://www.isc.org</a>   |
| • NLNETLABS                    | <a href="http://www.nlnetlabs.nl">http://www.nlnetlabs.nl</a>   |
| • DNSSEC.NET                   | <a href="http://www.dnssec.net">http://www.dnssec.net</a>   |

## ICANN Community Groups involved in DNSSEC:

- Commercial Stakeholders Group (CSG)
  - Commercial and Business Users Constituency (BC)
  - Internet Service providers and Connectivity Providers Constituency (ISPCP)
- Non-Commercial Stakeholders Group (NCSG)
  - Non-Commercial Users Constituency (NCUC)
- Security and Stability Advisory Committee (SSAC)

