DNSSEC *Securing the Internet*

Document available online at:
http://www.icann.org/en/news/in-focus/dnssec under "Factsheet"

ICANN
One World. One Internet
http://icann.org

Benefits to Companies and Consumers

What is it?

DNSSEC is a protocol that was 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[i], 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 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)

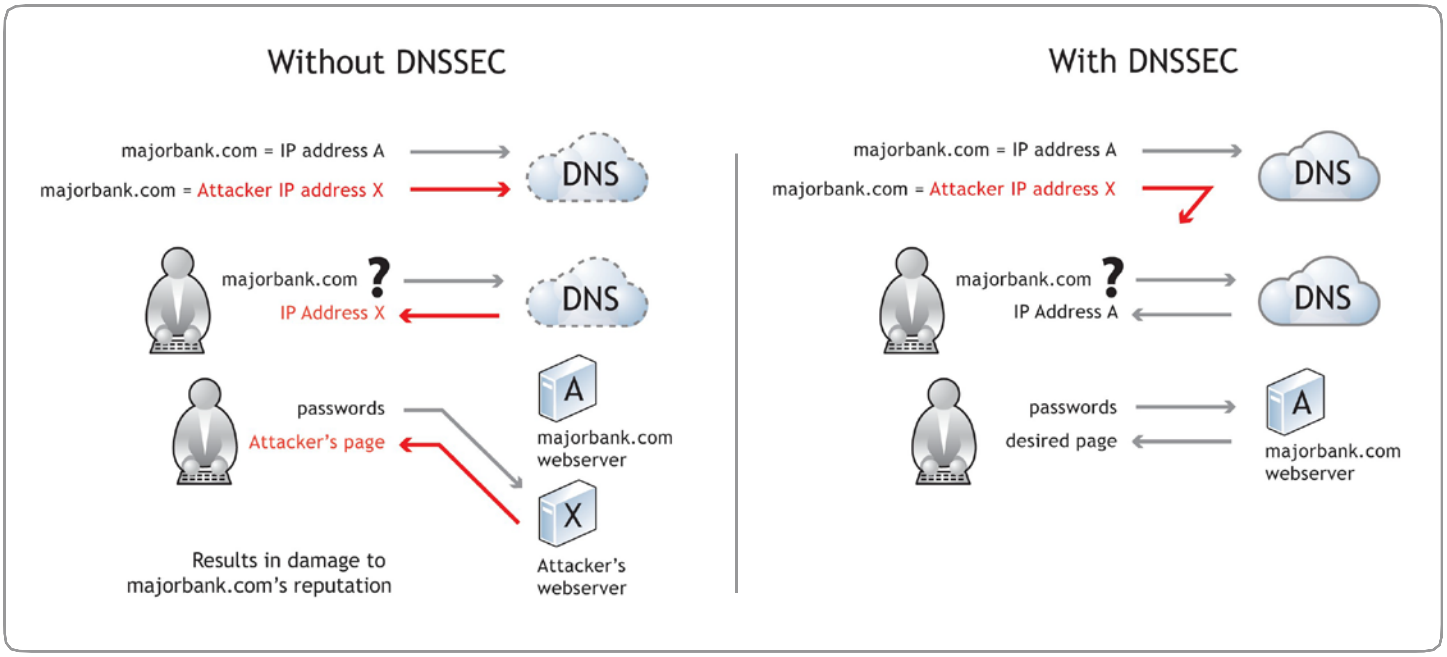
Deploy DNSSEC on corporate DNS infrastructure (turn DNSSEC validation "on" on your corporate DNS resolvers)

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 21 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., .se, .com, .рф, …etc)
- Educate and assist the Internet community regarding DNSSEC

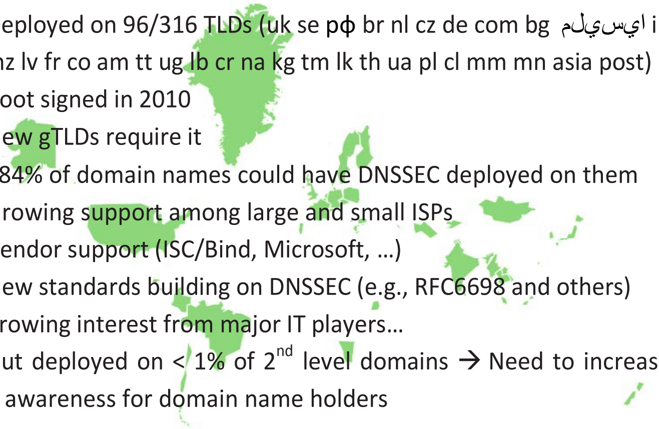


DNSSEC *Securing the Internet*

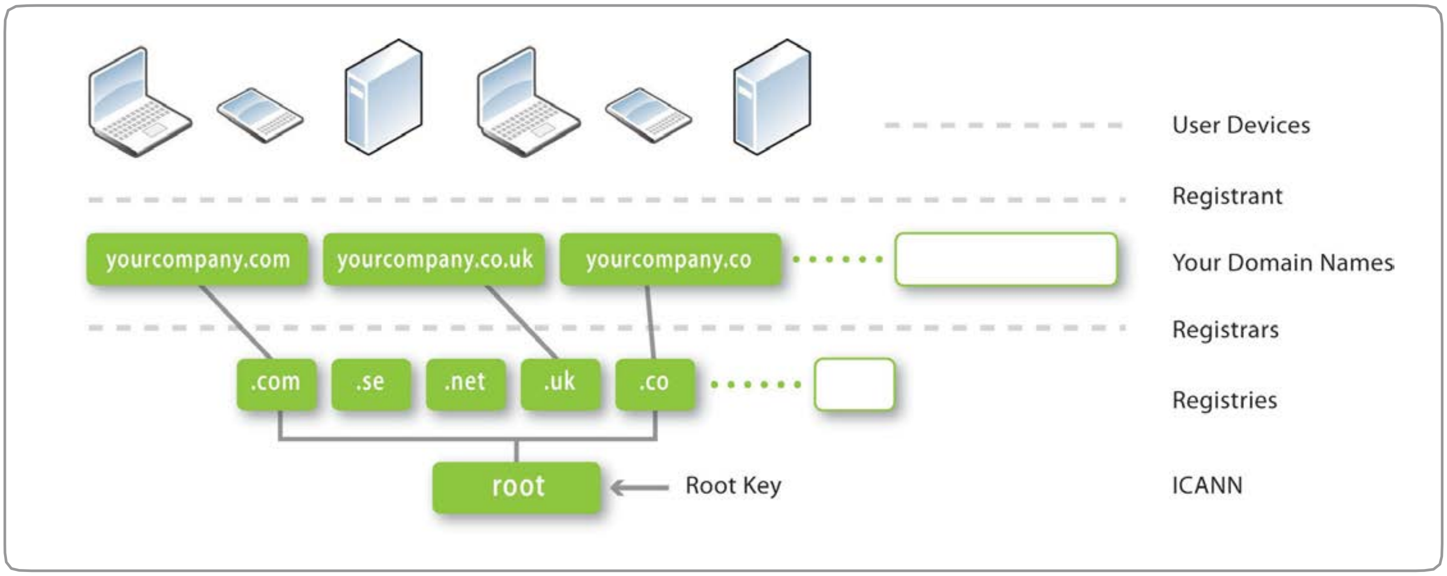
For Technical Advice:

• IETF	http://www.ietf.org https://datatracker.ietf.org/doc/draft-ietf-dnsop-rfc4641bis/
• ISOC Deploy360 Programme	http://www.internetsociety.org/deploy360/dnssec/
• DNSSEC Deployment Initiative	http://www.dnssec-deployment.org
• ISC	http://www.isc.org
• NLNETLABS	http://www.nlnetlabs.nl
• DNSSEC.NET	http://www.dnssec.net
• ICANN	http://www.icann.org/en/news/in-focus/dnssec

Status (28 Nov 2012):



- Deployed on 96/316 TLDs (uk se рф br nl cz de com bg مليسيا in jp nz lv fr co am tt ug lb cr na kg tm lk th ua pl cl mm mn asia post)
- Root signed in 2010
- New gTLDs require it
- >84% of domain names could have DNSSEC deployed on them
- Growing support among large and small ISPs
- Vendor support (ISC/Bind, Microsoft, …)
- New standards building on DNSSEC (e.g., RFC6698 and others)
- Growing interest from major IT players…
- But deployed on < 1% of 2nd level domains → Need to increase awareness for domain name holders



ICANN
One World. One Internet

http://icann.org

[i] DNSChanger: http://krebsonsecurity.com/2011/11/malware-click-fraud-kingpins-arrested-in-estonia/