IANA WG
DNSSEC

ccTLD TechDay

ICANN New Delhi 11th February 2008

Background

In July 2007, the ccNSO Council asked for input on Root Zone Signing : "the IANA Working Group is asked for help in providing input to the Council on Root Zone signing from a technical perspective."

IANA updates and investigations were presented in Los Angeles :
http://losangeles2007.icann.org/files/losangeles/presentation-ccnso-dnssec-survey-results-schittek-30oct07.pdf
http://losangeles2007.icann.org/files/losangeles/SigningRootZoneOlivier.pdf
http://losangeles2007.icann.org/files/losangeles/Lamb-DNSSEC_at_IANA.pdf

After discussion, we felt in the IANA WG that a general background discussion about DNSSEC was necessary, at least to agree on what the issue was ;

A drafting team was set up to write a paper within the IANA WG including IANA and including a limited set of relevant reviewers ;
Lesley Cowley (.uk),Olivier Guillard (.fr), Richard Lamb (icann), Oscar Moreno (.pr), frederico neves (.br), Shinta Sato (.jp), Gabriella Schittek (icann) and Roy Arends (.uk), Bart Boswinkel (icann), Ondrej filip (.cz), Jean-Philippe Pick (fr)

IANA WG PAPER

Organized into two parts:

Part I : DNSEC General background
Part II : Practical cases (including the root zone) and scenarios

Includes a comprehensive reference section about DNSSEC: 18 pointers, general paper on security to DNSSEC protocol specs, portals on DNSSEC, laboratory tests reports, and discussion on “Signing the root zone”;

Part I is drafted (IANA WG paper) and published on the ccNSO web site;

DNSSEC: the good things

DNSSEC consists of asymmetric cryptographic signatures included in the DNS, adding security features to the DNS: DNS information is signed before being published and (in principle) can't be faked anymore ;

DNSSEC protects information transported via DNS from possible corruption (even if the channel is not secured) ;

Therefore DNSSEC protects against some kinds of DNS abuse and, as such, can be a major DNS security improvement ;

DNSSEC : but

It would not be appropriate to say that DNSSEC "secures the DNS", since it doesn't solve all DNS security issues (Ddos attacks, outdated or misconfigured software);

DNSSEC requires the implementation of strict and rigorous general security policies in order to be usefully and effectively deployed : it may change registry organization quite significantly ;

DNSSEC introduces a significant increase of information circulating in the DNS (larger zones, larger responses) that may cause problems (overhead, bandwidth consumption, misinterpretation of DNS packets by certain [old] equipments) ;

DNSSEC CHECKLIST (draft)

Is it for me ? What should I look at ?

- ✓ Why DNSSEC Reputation ? Promote a more secure DNS ? Demand from my customers ? Opportunity for new services ?
- ✓ Is my Parent signed and ready to sign my KSK ?
- ✓ Do I want to announce DS for my customers ?
- ✓ Are there restrictions to access to my zone ? (do I need NSEC3)

DNSSEC CHECKLIST (draft)

Is it for me ? What should I look at ?

- ✓ Key management ?
- ✓ Zone Management and Zone Signing (zone update strategy ? Dynamic update ? Size of my zone ?)
- ✓ Do I need to upgrade my technical platform (overhead? bandwidth? EDNS0? etc)?
- ✓ Registry communication ? Legal implication ? Impact on internal operations ?

What's Next : HELP !

First Part ok : still couple of typos

To be done : provide an agreed « DNSSEC Checklist summary »
to help those that want to look at it

To be written : Part II (table of content drafted,
root zone signing section started: thanks Rick!)

Help IANA with testing: https://ns.iana.org/dnssec/status.html
(rollover, effective zone update including all parties, etc)

Contact:
ccnso-ianawg at icann.org
Olivier.Guiillard at nic.fr

QUESTIONS/COMMENTS ?

Volunteers ?