DNSSEC Deployment: A proposal for a half-day workshop at the APRIGF & SANOG meetings – August 2014 in Delhi

Prepared by
Don Hollander
Vo.2

APTLD proposes to hold a workshop focusing on the deployment of DNSSEC and the state of key issues in the community that are necessary for its success.

DNSSEC is a technology that will allow Internet users to be confident that the domain name that they are referencing is indeed the one that they are expecting. This is done through signing of the domain and each name space higher up in the name tree.

The Workshop will have the following components:

A Quick Look at the Technology, why it was developed, what it protects against and how it works • DNSSEC • DANE • Certificate Authorities	
A look at the players in the DNSSEC hierarchy – the role the play and what they need to do to make DNSSEC work:	
The Root • The root has been signed and all is good	
The Top Level Domain Registries • A look at the community of TLDs that are signed and their experiences and the ones that aren't signed and some inquire as to why they are not signed. Most of the gTLDs are signed, but not all of the ccTLDs are signed. • What efforts required to sign a zone?	
The Registrar • Registering signed names is effortful. How effortful will be covered	
The DNS Provider • Often, but not always, the ISP	
The Web or Mail Host • Where these are different from the Registrar or the DNS Operator	
The ISPs. • Both the ISP for the signed domain, but more importantly the ISP for the end user must support the service	
The End User • How will an end user know that a name is signed – and more importantly that a signed name is corrupt! Issues with browsers. • With the advent of the 'app', many end users never even see a domain name. How will the Apps know that their host has been hacked? • How will mail be shown as coming from a signed name – and more importantly that a signed name is not corrupt?	Ondrej Filip - .cz

The Early Adopters • The role of Governments, Banks and E-Commerce Sites	
The Future • Who needs to do what to get DNSSEC deployed – with particular focus on the Registry and the Community	