

A horizontal banner with a dark blue background. On the left side, there is a glowing blue globe with a grid overlay. The text "DNSSEC Deployment: Relevance for End-Users" is written in a large, white, sans-serif font across the center of the banner. In the background, there are faint, glowing lines and binary code (0s and 1s) suggesting a digital or network environment.

DNSSEC Deployment: Relevance for End-Users



James M. Galvin, Ph.D.
Director Strategic Relationships
and Technical Standards

jgalvin@afilias.info



First Principles

- An end-user needs a safe and secure Internet experience, with a readily visible and understandable indication that it is present
- The DNS is a critical Internet infrastructure component and securing it is both a natural evolution towards the next generation Internet and the cornerstone of secure Internet services today and those yet to be created
- This is not a technical presentation



What is DNSSEC?

- Using digital signatures it guarantees that the information you receive is the information that the owner wanted you to have
 - The IP address you asked for is the correct IP address
 - The email server you are about to hand off your message to is the correct email server
- The signed information is correct regardless of where you got it
 - The information is end-to-end secure



Why DNSSEC?

- Virtually everything we do on the Internet depends on the DNS
- The DNS is a critical Internet infrastructure component
- The DNS, both directly and indirectly, is an attack vector
 - Man-in-the-middle attacks mean that your web site or service can be hijacked
 - Phishing attacks are largely a social engineering vector but DNSSEC can provide some help



DNS Is All About Trust

- The DNS is fundamentally built on trust
- When you use your web browser to access your bank you trust that the web site you see is your bank
 - You trust your ISP, who did the DNS lookup on your behalf
 - You trust the registry who provided the IP address for the DNS to return to your ISP and then to you
 - You trust the root servers who told your ISP where to find the DNS for the registry you need to reach
- The really bad news: if there is a compromise at any point you have no way of knowing

Trust Is Not Enough

- End-users do not want to have to question whether or not it is a dog
- Enterprises want their end-users to know they are not a dog in disguise
- ISPs have a critical role in the identification of dogs
- Application and service providers who do not want to be confused with a dog need DNSSEC





Technical Tipping Point

- Since Sweden first signed in 2007 we now have about a dozen countries with signed zones and delegations
- .ORG was signed 2 June 2009 and will launch signed delegations in June 2010 – largest TLD to launch
- The root will launch signed delegations in July 2010
- .NET will launch signed delegations 4Q2010
- .COM will launch signed delegations 1Q2011
- If you are a TLD it is time to join the future
- If you are an enterprise you should have a plan



End-User: That is nice

- The average end-user has no idea what DNS is, so you can forget about DNSSEC
 - The average end-user has no idea what TLS/SSL is
- What an end-user does know is:
 - They are more secure when the address bar in their browser changes color
 - They are more secure when the padlock in the corner of their browser closes up
- We need a new color, or padlock, or something
 - The time is now



Challenge

- Enterprises who want to protect their brand and their market, who want to distinguish themselves as security leaders, need to sign their domains
- ISPs need to provide validating resolvers – check those digital signatures – to provide the safe and secure Internet that end-users expect, and assume they are getting



Opportunity

- Applications and services need to integrate DNSSEC so they can provide the visual cues that end-users need to be assured that they are safe and secure
 - Browsers
 - Email
- Because virtually everything depends on the DNS, it is the foundation upon which everything the user experiences is built, improving it – securing it – is an important evolutionary step for the Internet, for reasons we can not even imagine yet.



First Principles

- An end-user needs a safe and secure Internet experience, with a readily visible and understandable indication that it is present
- The DNS is a critical Internet infrastructure component and securing it is both a natural evolution towards the next generation Internet and the cornerstone of secure Internet services today and those yet to be created