.ASIA DNSSEC signing event
November 11, 2010
Verbal remarks
Dr. James Galvin
(please refer to DNSSEC presentation slide set at www.afilias.info/dnssec for visuals that correspond to these comments)

SLIDE 1:
Thank you Ching for that introduction. I am very pleased to be here today to discuss this important milestone not just for the .ASIA domain but for the Asian region as a whole.

SLIDE 2:
Afilias is .ASIA’s registry services provider and as such we provide both the registry database technology to enable registrations of new domains, but also the DNS system, which provides the address on the *highway* that Internet users travel to get from their computer to the website or Internet service they intend to reach.

Today, Afilias supports more top-level domains or TLDs than any other provider – 15 in total, across over 17 million registrations.

We are in the middle of the largest DNSSEC deployment across a registry system – signing more TLDs than any other service provider on the planet. We have dubbed this initiative Project Safeguard, which is illustrative of the importance Afilias places on safeguarding the billions of DNS transactions that cross our network each day. This week, we are focusing on our DNSSEC rollout in Asia-Pacific, benefiting the more than 840 million Internet users in this region.

My personal journey with DNSSEC began at an Internet Engineering Task Force meeting almost seventeen years ago and it is fitting that we are co-locating this event with the current IETF meeting. Serving as Chair of the first Working Group of the IETF to develop DNSSEC back in March 1994, we knew we had an important problem to solve to improve the DNS system as Internet usage worldwide started to accelerate.

SLIDE 3:
You, an average or maybe even a sophisticated Internet user, may not realize exactly how critical the DNS trust model is to the current situation you face in using the Internet to push and pull information on a daily basis.

Today when you visit a website, or send an email message, can you be sure you are communicating with the site or server that you think you are? The answer is No. At least not with certainty.

SLIDE 4:
The DNS protocol is an aging technology and even pre-dates the creation of the Web itself. Because its design was based on an inherent model of trust without the foreknowledge of the demands that would eventually be placed upon it and potential malicious things it would be used for, the DNS we know today lacks some key security features that, ideally, should have been baked-in from day one.

Today, the DNS simply accepts the first response it receives. Your web browser asks what is called an iterative resolver for a web site address. The iterative resolver asks the authoritative name servers in the DNS system for the web site address and it believes the first response it receives. It collects this response in its cache and it passes it on to your browser.

There is no inherent validation.

SLIDE 5:

DNSSEC adds a digital signature to the data elements in the DNS system to protect users from forged or hijacked data.

It does so by adding digital signatures to each response for the location of the website or email server you are trying to reach. So, if you ask for an IP address of a website, you get a signed response.

Similarly, if you ask for where to deliver email, you get a signed response. The iterative resolver checks and validates the signature to make sure you get the correct address.

SLIDE 6:

On this slide, I can show you how this works. You can see that the Internet user (or browser) is requesting to visit a website called trustus.asia. However a malicious actor wants to be that site, so they insert forged data into the resolver's cache so you get the wrong address. In addition, he sets up his server to masquerade as the real server when you connect to it, and none of this would be visible to you. You can see on the side the real trustus.asia server, not being used.

What is worse is that the forged data collects in a resolver's cache. A resolver caches the response so that it does not have to keep asking the authoritative name servers for the same information. It can respond more quickly to the next request it gets. This means the malicious actor only has to insert the forged response in the resolver one time, after which all users who ask for the same address will get the same forged response.

The average Internet user uses the iterative resolver of their local ISP. This means that once a malicious actor has gotten forged data into the resolver's cache, all users of that ISP will get a response with forged data when asking for the same web site.

SLIDE 7:

DNSSEC was developed as a solution to this problem. This new protocol, which has been in development for nearly two decades, enables cryptographic digital signatures to be added to the DNS data elements, allowing addresses to be automatically validated.

With DNSSEC, the DNS system uses a public-private key pair encryption mechanism similar to other systems already in wide use on the Internet. When a resolver requests DNS information about a domain name protected by DNSSEC, the response it receives is digitally signed using a private cryptographic key belonging to the domain's owner (shown here in green in the top-right corner). The resolver is then able to validate the signature using the domain's corresponding public key (shown here in yellow in the bottom-right corner). All this ensures that the user is then directed to the correct resource.

This means DNS resolvers, such as those used by ISPs can be certain that they send their users to the correct Web or email server. Due to its verifiable digital signatures, DNSSEC eliminates the possibility of DNS data being intercepted and fraudulently manipulated as it traverses the Internet.

We believe that DNSSEC lays a foundation of trust throughout the DNS system, where –in the future – consumers will be able to know with certainty that the website they are visiting is their inherent destination, and not a site that will steal their information, damage their computer, or steal their identity.

SLIDE 8:
There are a number of benefits of DNSSEC for many players in the industry.

For Registries, like .ASIA, they are demonstrating their leadership and commitment to a safer and more secure Internet by deploying the latest in security standards that will be the requirement for the future. .ASIA is laying the foundation of a new level of trust to empower the development of a new generation of security technologies that application and service providers can rely on to enhance the Web and the Internet for decades to come.

For registrars, or the retailers from whom website owners buy their domain names, this allows them to provide enhanced security services to their customers, even perhaps going as far as premium product offers.

Of course for site owners, or registrants, there is the benefit of enhanced trust that their customers will have when visiting their websites.

And finally for end-users, this trust is paramount. Imagine a user attempting to access their bank online – the power of knowing the site they are visiting is the correct site and not a potential malicious actor is tremendously important.

SLIDE 9:
As I mentioned the DNSSEC effort is nearly 2 decades old. The protocol itself began developing in 1993. However in recent years it has gained momentum with .ORG’s deployment of signing its zone in 2009, and then full production deployment in 2010. Also this year in July the Root was signed, enabling resolvers to validate DNSSEC TLDs through the regular Internet we all use every day.

Of course now we are in the midst of Afilias’ Project Safeguard and our deployment of DNSSEC across 13 more of the TLDs we support including .ASIA.

In late 2010 and early 2011, we also expect .NET and .COM to be signed.

SLIDE 10:
Current developments across the “chain of trust” are turning the tide on the demand for DNSSEC. Major TLDs have signed, 53 TLDs at last count. The root is signed.

The incentives of deployment now outweigh the barriers and it is now time for ISPs and application and service providers to get on board with deployment.

In the future, DNSSEC will enable Internet users to enjoy unprecedented levels of trust when they communicate or transact online. Because DNSSEC is handled entirely "in the cloud", for the average Web user, the changes will at first be mostly transparent. But we hope to be able to work with other important members of the chain of trust to ensure they are DNSSEC-aware, enabling the security benefits of signed domains to be conveyed to users in much the same way as SSL-encrypted Web pages are today. DNSSEC is not just about protecting the DNS; it is about what we will do with it as a result of empowering the development of a new generation of security technologies that will result in a safer, more secure Internet for decades to come.

SLIDE 11:
Thank you