DNSSEC Workshop

http://brussels38.icann.org/node/12491

Wednesday, 23 June 2010 – 09:00 – 13:30

[2010-06-23 09::05:16] DaveP: i think Olaf could make better distinction of roles to emphasize the need for a distinct technical administrator contact

[2010-06-23 09::05:53] markus: Hi Dave, would you like to comment on Olafur after his presentation?

[2010-06-23 09::06:06] DaveP: i'm in the room:-)

[2010-06-23 09::06:10] markus: OK

[2010-06-23 09::06:20] DaveP: but far from a mic so here is the point i'd make

[2010-06-23 09::06:47] markus: Please raise your hand or go to a mic. I think your point is valid

[2010-06-23 09::08:59] DaveP: what I would want from a registrar is the ability to "configure" my registration so that I can identify (a) someone in my organization who has write permissions on DNS in three distinct scenarios (1) I operate name service in house, (2) my registrar is my name service provider, and (3) a 3rd party (not me or my registrar) is my name service provider

[2010-06-23 09::09:17] CSC_2: what is the recommended time to keep a zone alive after transfer of DNS to a new provider?

[2010-06-23 09::10:17] DaveP: (b) I want to delegate to my registrar or a 3rd party for the same 3 cases (1-3)

[2010-06-23 09::10:30] Doug_Barton: CSC_2, the general BCP is 2 x TTL of the longest record

[2010-06-23 09::10:33] DaveP: this technical administrator should receive confirmations and notifications from the registrar

[2010-06-23 09::10:48] markus: dave I'll take care of your point if that's OK

[2010-06-23 09::14:59] markus: Dave, I hope I made the point you wanted to make

[2010-06-23 09::15:20] ICANN_Camera13416: Markus: Please ask the cameraman to leave the front row.

[2010-06-23 09::15:27] DaveP: yes you did thank you!

[2010-06-23 09::16:25] markus: Is everything working with the camera again

[2010-06-23 09::16:43] ICANN_Camera2775: Yes Dan, thank you.

[2010-06-23 09::17:33] DaveP: someone take a snapshot of Kaminsky in a suit quick!

[2010-06-23 09::17:49] Jorge19457: looks like he got a job to buy a tie

[2010-06-23 09::20:44] Doug_Barton: Anyone want to take a side bet on whether or not he mentions DLV?

[2010-06-23 09::22:37] Jimmy: Is there a timeline on adding DS keys from TLDs in the root? Some big TLDs, like .EU, are ready.

[2010-06-23 09::23:37] Doug_Barton: Jimmy, it was just announced a few minutes ago that it was already starting

[2010-06-23 09::23:51] markus: I guess this is a good question for the last presentation on the status of the root zone. You have to wait until 1pm however

[2010-06-23 09::24:08] markus: Yes, there are already some TLD DS records in the root

[2010-06-23 09::24:26] bertPowerDNS: uk

[2010-06-23 09::25:21] Doug_Barton: markus, one question and one observation .... question, how is this better and/or easier than asking R/Rs to support DS? Observation, there is no such thing as "sunset period" for this kind of stuff, once it's in, it's in

[2010-06-23 09::25:29] Jorge19457: greedy people are a risk to DNS, beaware Rod is listening you may be in line for the pee-pee test now

[2010-06-23 09::25:51] ch: How is NSDS supposed to work when a lot of registry/reseller web interfaces do input validation?

[2010-06-23 09::28:59] ¬ª sean_ is now known as SeanPowell.

[2010-06-23 09::30:33] Doug_Barton: *tap tap* Is this thing on?

[2010-06-23 09::30:48] DaveP: be patient:-)

[2010-06-23 09::30:51] Jimmy: About the question being asked now: isn't that the task of the resolver?

[2010-06-23 09::30:57] Doug_Barton: oh, cool, thanks :)

[2010-06-23 09::31:46] CSC_2: Dan - can you speak to your sense of increased risk of impact of DoS attacks due to the larger packet sizes resulting from DNSSEC?

[2010-06-23 09::32:43] bob: RoyArends: With this nsds hack, we need to rename our nameservers everytime we roll the key. Too much hackery, extremely little value.

[2010-06-23 09::34:38] markus: I guess this idea is still somewhat controversial

[2010-06-23 09::35:01] Doug_Barton: Oh, apparently I didn't understand the proposal ... he seems to be suggesting that registries take this nsds things and extract the DS record without the registrar's direct involvement?

[2010-06-23 09::35:18] markus: Yes, doug, that's the way I understood it

[2010-06-23 09::35:23] Doug_Barton: Oh, sorry

[2010-06-23 09::35:43] markus: Never mind, I guess clarification is a good thing

[2010-06-23 09::36:06] CSC_2: NSDS would be a means to insert DS records into the regisitry TLD root zone without having to implement EPP extensions for SEC

[2010-06-23 09::36:18] Doug_Barton: I can't imagine that any gTLD registry would ever implement this, and I'd be surprised if any useful subset of ccTLDs would do it either

[2010-06-23 09::36:20] markus: You are right

[2010-06-23 09::36:48] bob: Holdon, csc_2, I thought there would still need to be a change on the epp code anyway, according to Dan's slides.

[2010-06-23 09::36:51] Jimmy: DNSSEC is already a large adoption and change for all levels, don't forget that stuff needs to be actually validated by the resolvers too. I don't think it's wise to introduce yet another way to speed up things (NSDS proposal). Shouldn't we just have a little more patience?

[2010-06-23 09::36:52] Doug_Barton: CSC_2, thanks ... sorry I'm so slow on the uptake :)

[2010-06-23 09::37:07] bob: YES,

[2010-06-23 09::37:39] Doug_Barton: also, if there is real demand for DNSSEC market forces will take care of getting the registrars on board

[2010-06-23 09::37:46] ch: Even if someone would implement that, they would need to track who's using that, etc. and cause large impact on the registry side...

[2010-06-23 09::38:59] CSC_2: Dan mentioned that the registry would need to update their EPP parsing in order to translate NSDS into DS

[2010-06-23 09::39:23] Jimmy: Basically I don't trust registrants / DNS operators to just pass on information that we, as a registrar, just send to the root. I don't see how efficient validation is possible here, this goes beyond just "character" validation.

[2010-06-23 09::39:47] Jimmy: *to the root -> *to the registry

[2010-06-23 09::40:16] ch: Registries would also need to return NSDS to registars, _if_ they've ever used it, and then at some point convert all to NS+DS when the registrar is doing proper NS+DS

[2010-06-23 09::42:09] Jimmy: I don't like the idea. I think this is going to add a lot more confusion and conversion work. Dan was right that DNSSEC isn't that hard, but it's something entirely new for a LOT of people, we're going to have enough work evangalizing it (not only to the common man, but also to resellers that want the technical info).

[2010-06-23 09::43:36] CSC_2: I don't believe that NSDS is a concern for Registrant/DNS Operators but rather somewhat of a transport means for Registrars...

[2010-06-23 09::46:00] Doug_Barton: here here Jim

[2010-06-23 09::46:01] Jimmy: Jim Galvin is right.

[2010-06-23 09::49:15] CSC_2: Panel - given that many Registrars terminate hosted DNS when a domain is transfered out or delegation away AND if it is imperative that DNS stay alive on the losing DNS servers, what can be done to develop policy and then enforce?

[2010-06-23 09::50:07] Doug_Barton: This whole area is an ICANN PDP waiting to happen

[2010-06-23 09::50:55] Jimmy: Jim is right when he says that the zone should be easily exported, for the purposes of moving a domain name, but this should really be an explicit request. I don't want to bombard registrants with RRSIG, DNSKEY, NSEC3, ... records. DNSSEC may look clear to us, but the end user is just the "common internet users" who typically have a very basic understanding of DNS. To move things along, there are some things that need to happen transparantly and worry-fre

[2010-06-23 09::53:25] CSC_2: Panel - given that many Registrars terminate hosted DNS when a domain is transfered out or delegation away AND if it is imperative that DNS stay alive on the losing DNS servers, what can be done to develop policy and then enforce?

[2010-06-23 09::57:23] Jimmy: Panel: There's another level in the domain name model, the reseller. You have the registry, registrar, reseller and the registrant. So for the registrar, there might be two underlying levels to deal with. Don't you agree that this will require a lot of effort of the registrar evangalizing this to both levels? I'm asking this because I feel a consensus, mostly from Dan, that DNSSEC is easy-peasy. It's might not be technically, but it surely is on the market

[2010-06-23 09::58:28] Jimmy: Last sentence should have been: "It might be technically, but it surely isn't on the marketing / political section."

[2010-06-23 10::01:33] markus2: Had some network problems. I am sorry if I missed any questions

[2010-06-23 10::01:54] Jimmy: Markus: did you see mine?

[2010-06-23 10::02:33] Hugo_Salgado: I have a question to the registrars here that already implemented dnssec for their clients. Did you found it necessary to increase the security level in the identification of your customers? Lets say, using digital certificates, not only a login/password, to be able to pass DS data?

[2010-06-23 10::03:14] markus2: No, I am sorry, please repeat. I have been apparently disconnected after 9.42 but I didn't see it on my screen

[2010-06-23 10::03:39] CSC_2: ..the chain of trust is only as strong as the weakest link. Therefore, the communication from registrart to registrar must occur over secure channels.

[2010-06-23 10::03:43] Jimmy: Markus: Panel: There's another level in the domain name model, the reseller. You have the registry, registrar, reseller and the registrant. So for the registrar, there might be two underlying levels to deal with. Don't you agree that this will require a lot of effort of the registrar evangalizing this to both levels? I'm asking this because I feel a consensus, mostly from Dan, that DNSSEC is easy-peasy. It might be technically, but it surely isn't on the m

[2010-06-23 10::04:03] CSC_2: QUESTION - given that many Registrars terminate hosted DNS when a domain is transfered out or delegation away AND if it is imperative that DNS stay alive on the losing DNS servers, what can be done to develop policy and then enforce?

[2010-06-23 10::09:34] DaveP: is it necessary for all registrars to support DNSSEC? if a registrar concludes the cost is prohibitive and it's too hard and my software vendor can't deliver it, who is affected other than the registrar? A registrant who wants DNSSEC but cannot get it from his current registrar may incur some overhead for transferring domains, but is there any other adverse affect?

[2010-06-23 10::09:52] Jimmy: Last speaker: The registrars have A LOT more data to sign in some cases, the challenge is bigger! You only have a few records per domain name!

[2010-06-23 10::10:54] CSC_2: follow question to DaveP: when does .SE intend to require Registrar's to support DNSSEC as a requirement for domain transfers?

[2010-06-23 10::16:38] markus2: @CSC_2 I think you are raising an important point about policies and ways of enforcing them. I know Olafur is working on possible concepts for policies as are some registries. However, at this stage most of the discussion is still about explaining the problem of transfers

[2010-06-23 10::20:21] CSC_2: to me, the trend in the market place is for Registrars being more and more aggressive in termination of DNS...not a trend toward coorporation. In order to alter this trend, significant work must be done by ICANN and Registries.

[2010-06-23 10::21:24] DaveP: I have this sense of deja vu - more than a decade ago, emerchants deliberated whether to support SSL or process payments offline. Some decided certs cost too much, SSL slowed down transactions, etc. Roll forward a decade. How prevalent is that attitude? Not prevalent at all. I think the "innovate or die" comment is spot on.

[2010-06-23 10::23:18] markus2: Yeah, we have a very full programm. I am sorry not to be able to put all the issues forward mentioned in this chatroom

[2010-06-23 10::23:50] CSC_2: @DaveP - agreed. As a registrar, we don't see this as an option. I don't see that a traditional revenue calculation can be made to validate the business case. Rather, it is to positioned as 'the cost of doing business'

[2010-06-23 10::24:03] markus2: However, I do think this online discussion is really valid and there are about 35-40 people listening to it

[2010-06-23 10::25:56] markus2: Yes, but I am a real fan of online participation since I believe the ICANN community can be tremendously expanded by using it effectively

[2010-06-23 10::27:40] lightIRC_5493: Heh all, this is Dan Kaminsky. Please let me apologize for the out of date slides at ICANN's site. NSDS slides at recursion.com/chain.pdf

[2010-06-23 10::28:21] CSC_2: @Dan - do you see an increased risk of impact of DoS due to the larger packet sizes due to DNSSEC?

[2010-06-23 10::28:22] DaveP: CSC_2, you're absolutely correct. DNSSEC will be a given at some future time, whining about having to do it is not very productive.

[2010-06-23 10::29:06] Dan_Kaminsky: @CSC_2 -- No, DoS is perfectly doable without needing DNSSEC

[2010-06-23 10::29:27] CSC_2: denial-of-service attacks...sorry

[2010-06-23 10::29:33] Dan_Kaminsky: @CSC_2 -- Fixing DoS is basically orthogonal from DNSSEC

[2010-06-23 10::30:21] CSC_2: understood - but since the packets are necessary larger (for DNSSEC), ought the risk of impact increased?

[2010-06-23 10::30:56] DaveP: one "value add" DNSSEC offers to DDOS attackers is the ability to amplify without creating relatively easy "big responses" using TXT or other response packets

[2010-06-23 10::31:13] Dan_Kaminsky: @DaveP Yeah, emphasis on relatively easy :)

[2010-06-23 10::32:23] DaveP: no matter what you use in your amplified response, the countermeasure will still be some detection or filtering of the pattern

[2010-06-23 10::33:09] Dan_Kaminsky: @DaveP There's some work going into detecting that one is part of a flood. It's gong to require some interesting work

[2010-06-23 10::34:12] DaveP: the whining about DNSSEC facilitating DDOS is just that. whining.

[2010-06-23 10::35:45] CSC_2: would you characterize the sentiment from the security communicty is that the risk of potential increased impact (DDoS) is minimal compared to the value of a secure DNS?

[2010-06-23 10::38:11] DaveP: @CSC_2 I think you have to consider comparative risks, consider whether you have a countermeasure for each risk, how effective the countermeasures are, and which of the risks ends up being "greater"

[2010-06-23 10::38:44] Dan_Kaminsky: @CSC_2 I'd say the overall security community remains somewhat skeptical. Deployment numbers remain small. But certainly DoS from DNSSEC doesn't get much cred

[2010-06-23 10::39:06] Dan_Kaminsky: @CSC_2 Remember, DNSSEC touches a lot of things we've heard for *years* would finally work

[2010-06-23 10::40:26] CSC_2: thanks, Dan/Dave

[2010-06-23 10::40:48] DaveP: @Dan - our track record with security protocols is pretty sad. I don't know of any we've deployed that satisfy the security community so I'm not surprised at the skepticism

[2010-06-23 10::42:37] DaveP: @Dan - that being said, I think adoption has been beneficial. I just wish we would apply what we've learned from past adoptions faster and more consistently.

[2010-06-23 10::56:06] CSC_2: @Dan - from a security persective, do you have comment on time/frequency of DS rollover?

[2010-06-23 11::01:12] RoyArends: It is less complicated than an SSL implementation. It is less complicated than an SSH implementation.

[2010-06-23 11::08:40] CSC_2: @Hubert - will PowerDNS support ZSK's 'per zone' rather than 'per server' ?

[2010-06-23 11::12:02] Ed_van_der_Salm: Is there a mixed mode, plain-text files (bind-mode) and a database, for easy migration?

[2010-06-23 11::14:00] CSC_2: nice

[2010-06-23 11::14:07] esthermakaay: ed: you can run mixed

[2010-06-23 11::14:13] Ed_van_der_Salm: tx

[2010-06-23 11::14:18] esthermakaay: 3.0... when it is ready

[2010-06-23 11::14:36] klaus: :)

[2010-06-23 11::14:42] Ed_van_der_Salm: ok, will wait till sidn signes .nl

[2010-06-23 11::14:44] klaus: no roadmap?

[2010-06-23 11::15:09] esthermakaay: 'few weeks

[2010-06-23 11::17:07] bertPowerDNS: hi!

[2010-06-23 11::17:57] fneves: Bert congrats, nice work. Large hosting providers of small zones thank you!

[2010-06-23 11::18:18] markus: test

[2010-06-23 11::18:48] CSC_2: @Nominet - when do you expect to release updates to your EPP implemtation? Do you intend to _require_ Registrars to implement DNSSEC?

[2010-06-23 11::20:05] bertPowerDNS: fneves: thanks

[2010-06-23 11::28:15] Olafur: Another victim of the freqent rollover syndrome, there is no need to roll 2048 bit KSK that frequently

[2010-06-23 11::28:52] CSC_2: @Olafur - what frequency do you recommend?

[2010-06-23 11::29:50] Olafur: KSK only roll when you upgrade/replace your HSM

[2010-06-23 11::41:17] CSC_2: @Panel - do any of you intend to require Registrars to implement DNSSEC?

[2010-06-23 12::26:39] Guest_216688: pong

[2010-06-23 13::09:41] CSC_2: hello?

[2010-06-23 13::09:57] Ed_van_der_Salm: anybody here?

[2010-06-23 13::10:37] Marcus_Jaeger: did everyone run away

[2010-06-23 13::11:32] CSC_2: don't hear anyone on the dial-in phone line either...

[2010-06-23 13::12:07] Ed_van_der_Salm: Yep, looks like it...

[2010-06-23 13::12:13] SeanPowell: they're still at lunch it appears

[2010-06-23 13::15:42] Ed_van_der_Salm: Don't forget the sound please...

[2010-06-23 13::20:07] Ed_van_der_Salm: Nobody here yet?

[2010-06-23 13::20:31] Ed_van_der_Salm: I thought I saw people sitting down?

[2010-06-23 13::20:54] ICANN_Camera2775: not starting just yet

[2010-06-23 13::21:01] Ed_van_der_Salm: tx

[2010-06-23 13::27:34] Ed_van_der_Salm: Is it me, or is there no sound?

[2010-06-23 13::28:14] CSC_2: I hear nothing

[2010-06-23 13::28:44] ICANN_Camera2775: working on it

[2010-06-23 13::31:00] Ed_van_der_Salm: The camera is not changing also

[2010-06-23 13::32:29] Ed_van_der_Salm: reload is the solution, sound and video working

[2010-06-23 13::49:37] Hugo_Salgado: Question: how the root key will be "uncovered"? As a rollover from the covered key? Or just changing it simultaneously on every root server?