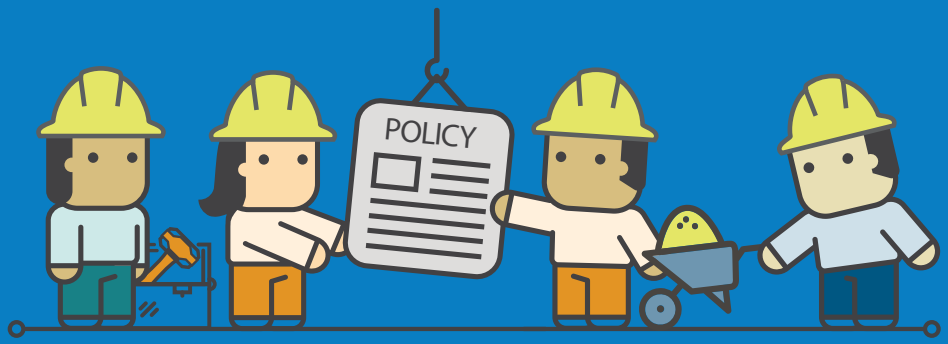
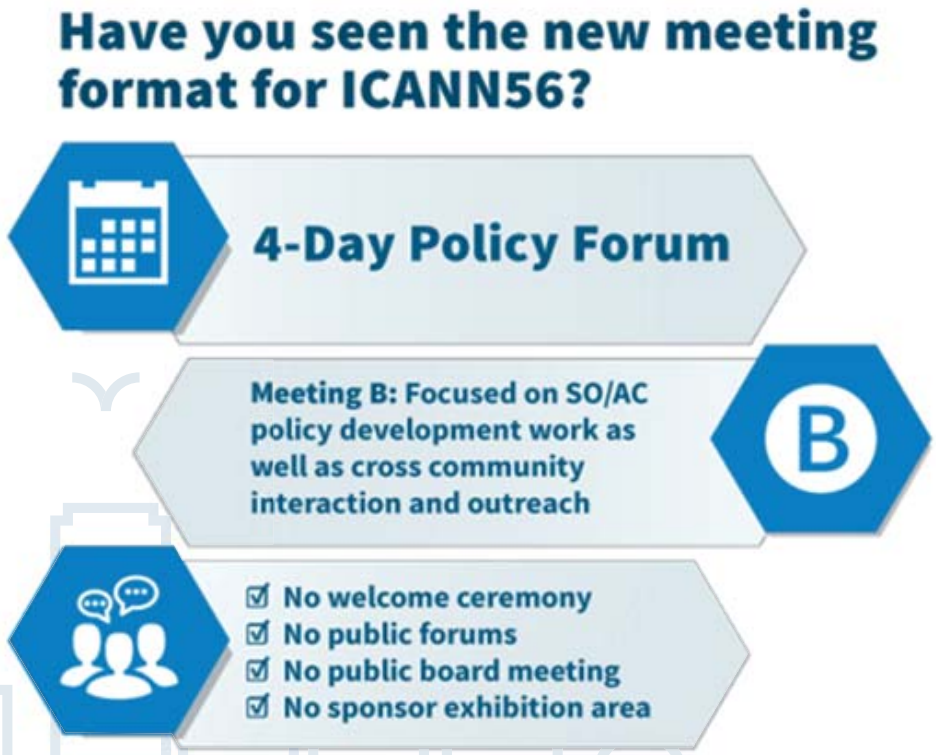
ICANN|56
HELSINKI
POLICY FORUM
27-30 JUNE 2016

RELATÓRIO DNS.PT

ÍNDICE



Esta edição da ICANN, que decorreu em Helsínquia entre os dias 27 e 30 de junho, inaugurou um novo formato de funcionamento ao nível dos três encontros públicos anuais da comunidade envolvida. Naquela que seria supostamente a reunião digamos, menos expressiva, do ano, não só em termos de duração como também de participantes, estiveram presentes mais de 1400 participantes. Esta foi também a primeira reunião em que Göran Marby participou enquanto presidente e CEO da ICANN. O modelo desta reunião, doravante designada de Policy Forum, resume-se no seguinte esquema:



Prémio Multistakeholder Ethos

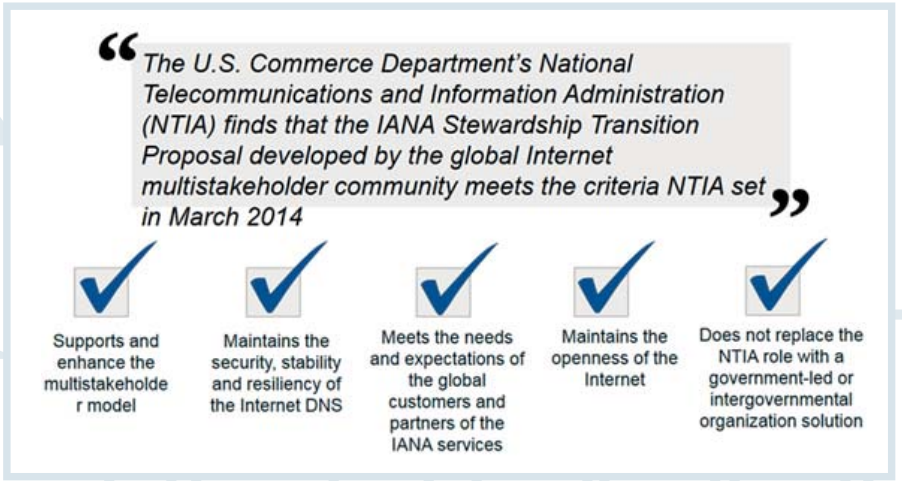
Em 2014 foi lançado no âmbito da ICANN 50 em Londres, o Prémio Multistakeholder Ethos que visa reconhecer participantes da ICANN que, de forma notória e amplamente reconhecida pela comunidade, têm contribuído para a implementação do modelo multistakeholder. A existência deste prémio reflete a relevância dada pela ICANN a este modelo multiparticipativo sobre o qual deve assentar a governação da Internet. Da lista de 19 nomeados foram este ano selecionados o americano Chuck Gomes e o neozelandês Keith Davidson.

Mais informação em:
https://www.icann.org/news/announcement-2016-06-27-en

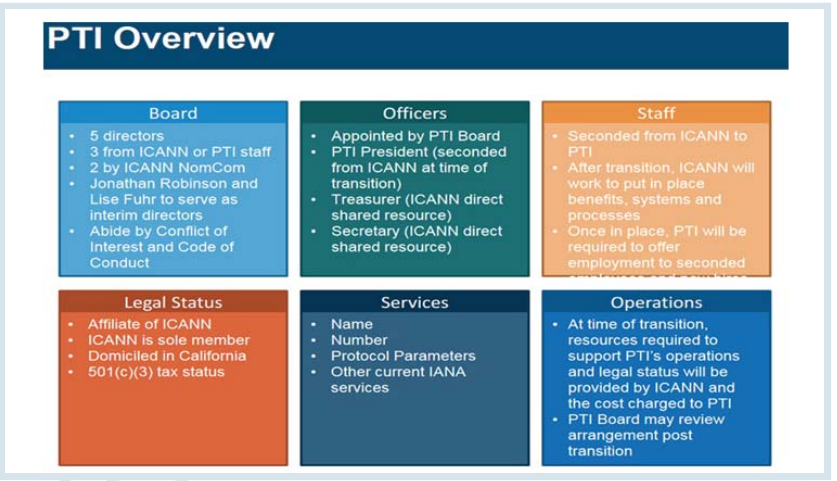
Processo de transição das funções da IANA

Considerando que o contrato com a NTIA cessa já no próximo mês de setembro, neste momento os assuntos mais críticos estão centrados na criação dos estatutos da chamada PTI (Post Tansition IANA), definição do respetivo modelo de funcionamento, staff e redação dos termos e condições a verter no contrato a celebrar com a ICANN. Entretanto há um conjunto de princípios que se entendem como fechados, a PTI (ainda sem designação social) será uma instituição sem fins lucrativos, estabelecida à luz da lei Californiana, à semelhança de resto da ICANN. Em termos de membros fundadores, a ICANN será o único. O contrato a firmar terá por base o já atualmente em vigor, incorporando as propostas do CWG, estará limitado aos nomes, e incluirá disposições muito concretas em termos de níveis e qualidade de serviço.

No passado dia 10 de março na sequência de um processo de longa discussão que se prolongou, a nível mais formal, desde meados de outubro, foi submetida à NTIA a proposta da ICANN, da qual resultou a comunicação pública que se passa a reproduzir:



O futuro da PTI perspetiva-se com um contexto próximo desta realidade:



Modelos de governação

O .UA, ccTLD da Ucrânia, fez uma breve apresentação sobre a sua estrutura de funcionamento, disponibilizando aos presentes um conjunto de dados sobretudo direcionados ao seu modelo de negócio. Atualmente com cerca de meio milhão de domínios registados, com uma taxa de renovação de 94% e com 119 registrars, este ccTLD, cuja delegação remonta já há 24 anos, é gerido por uma entidade privada – www.hostmaster.ua - , tendo já implementado os IDN, EPP e DNSSEC.

No passado dia 4 de maio o registry do ccTLD .nz – InternetNZ – e o governo da Nova Zelândia, na pessoa do seu Ministro das Comunicações, assinaram um memorando de entendimento cujo objetivo primeiro foi, na prática, o de formalizar o que há muito vinha a ser garantido por este registry, com uma gestão transparente e que defende os interesses da comunidade Internet local. Com a assinatura deste MoU pretendeu-se fazer face a três particulares questões que regularmente eram chamadas à colação: o possível impacto do desenvolvimento de políticas discordantes entre o registry e o governo, a definição da natureza dos lucros do registry que não podem ser tratados como, por exemplo, receitas de impostos e, por fim, o facto de não existir qualquer tipo de documento formal que regulasse a relação do governo e do registry no âmbito da gestão do ccTLD nacional.

Tratou-se de um processo negocial iniciado pelo registry e que assentou numa abordagem aberta e multistakeholder. As negociações decorreram durante 18 meses e o grupo de trabalho foi composto por três membros do .nz e pelo representante da Nova Zelândia no GAC e o resultado final acabou por, no entendimento dos primeiros, legitimar a sua atividade e linhas gerais de ação. O MoU[1] teve por base grande parte dos princípios gerais plasmados no RFC 1591, a saber: o mercado dos nomes de domínio deve ser competitivo; os registrants devem ter absoluta e plena liberdade de escolha; deve operar um modelo de first come, first served; os dados dos registrants devem ser públicos e as políticas aplicáveis ao TLD devem ser determinadas na sequência de processos abertos e multistakeholder.

O MoU acabou por definir o papel de cada uma das partes na gestão do ccTLD. Em concreto ao governo cabe agora a responsabilidade de assegurar que o registry cumpre o RFC1591, sobretudo ao nível da estabilidade, resiliência e segurança do DNS. Para a InternetNZ aquilo que eram as suas práticas correntes de gestão assumiram agora o estatuto de obrigações formais: gestão transparente com a publicação dos relatórios anuais de gestão e contas e realização de processos de consulta aberta aquando da realização de eventuais alterações a políticas aplicáveis ao registo de .nz. Surgiu no entanto uma nova obrigação direcionada em exclusivo ao registry: "*(...) regularly testing views of the broad community (...)*".

[1] *https://www.icann.org/sites/default/files/assets/iana-stewardship-timeline-10mar16-en.pdf*

Daqui vai resultar que o registry tem de criar mecanismos que lhe permitam identificar as reais necessidades da comunidade Internet local tentando, dentro do seu âmbito de atuação e meios disponíveis, fazer-lhes face.

O MoU já entrou em vigor, mas, tendo em consideração o apresentado pelo registry InternetNZ e aduzido anteriormente, os próximos meses não ditarão particulares novidades na gestão do .nz.

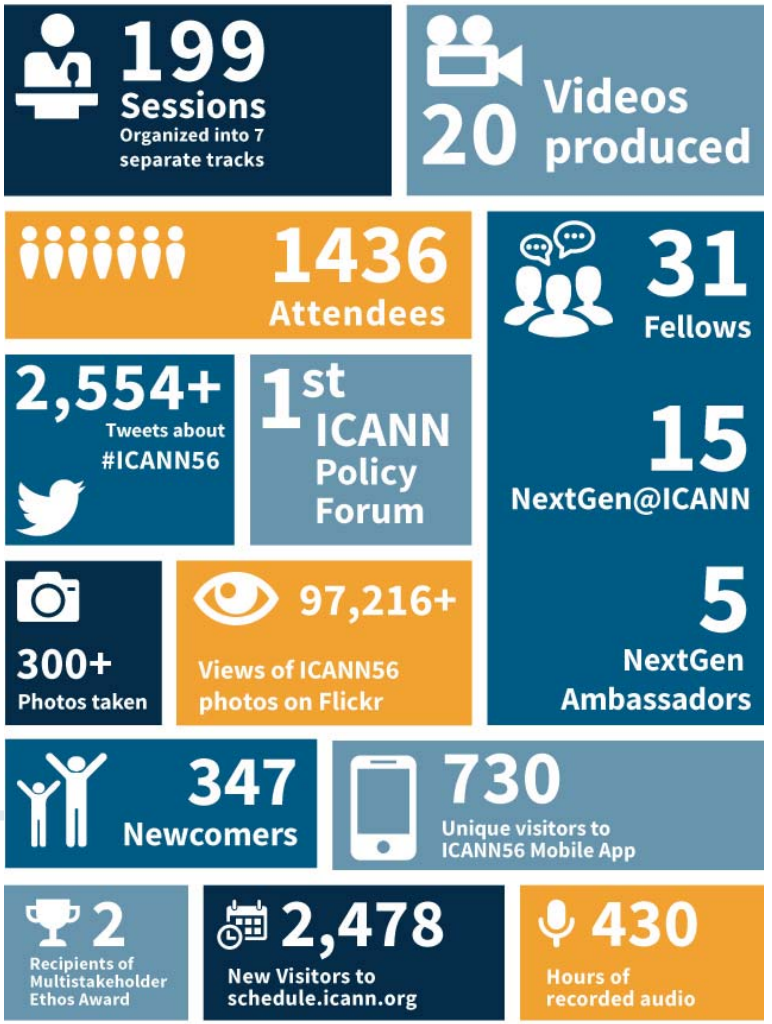
Lista de acrónimos:
https://centr.org/education/acronyms.html

Relatório do CENTR:
https://centr.org/library/external-event/centr-report-on-icann56.html

GAC communiqué:
https://gacweb.icann.org/download/attachments/27132037/20160630_GAC%20ICANN%2056%20Communique_FINAL%20.pdf?version=1&modificationDate=1467306358279&api=v2

ICANN pelo mundo:

ICANN 56 em números:



ICANN | 56 • TECH DAY

A sessão *TechDay* da 56ª reunião do ICANN em Helsínquia decorreu na manhã de segunda-feira. Ao contrário do que é habitual, esta sessão teve uma duração de apenas uma manhã devido ao novo formato das reuniões do ICANN. Os temas apresentados foram os seguintes.

Host Presentation - Juhani Juselius, FICORA

A sessão abriu com uma breve apresentação de *Juhani Juselius*, o responsável pela gestão do *Registry* FICORA que gere o ccTLD da Finlândia, o .FI, e a organização anfitriã da 56ª reunião do ICANN. o .FI tem atualmente cerca de 390.000 domínios, com uma taxa anual de crescimento na ordem dos 5.5%, 12 colaboradores a tempo inteiro, e onde opera no modelo *Registry/Registrar* tal como no DNS.PT. Suporta o registo de domínios com caracteres especiais, mais conhecidos por *Internationalized Domain Names* (IDN's), IPv6 e DNSSEC. A infraestrutura de servidores de nomes do .FI é composta por 8 servidores de nomes autoritativos, nomeados alfabeticamente de "a.fi" a "h.fi". Destes 4 são nuvens *Anycast* (vários servidores de nomes distribuídos geograficamente a responder por um único nome e endereço IP), e os restantes 4 são servidores em *Unicast* (uma única localização).

A destacar, as grandes alterações que irão ser introduzidas já no próximo dia 5 de setembro deste ano, sobretudo na componente do regulamento de registo de domínios, e no modelo de operação, tornando-se uma entidade *Registry* em exclusivo. Segundo o responsável do .FI, esta é uma tentativa do .FI se aproximar dos *Registrars* que trabalham com o .FI, para assegurar a sua posição no mercado DNS, cada vez mais aberto.

Zonemaster - Mats Dufberg, IIS

Mats Dufberg, do Registry IIS responsável pela gestão do ccTLD da Suécia, o .SE, apresentou a ferramenta Zonemaster. Trata-se de uma ferramenta de avaliação técnica de domínios, capaz de realizar mais de 60 testes distintos, desenvolvida no modelo *opensource* em estreita colaboração pelos *Registries* IIS (.SE) e AFNIC (.FR). Este projeto surgiu para substituir as anteriores ferramentas *DNSCheck* e *Zonecheck*, iniciou em 2013 e dois anos depois, ficou disponível online download e utilização. Em suma, é uma ferramenta muito completa e robusta.

.NZ Registrar Portal - Jay Daley, InternetNZ

Jay Daley do Registry InternetNZ responsável pela gestão do ccTLD .NZ correspondente à Nova Zelândia apresentou o novo portal para os *Registrars* de domínios .NZ, ainda em desenvolvimento. Este portal é baseado em conceitos de *Business Intelligence* (BI), e apresenta-se como uma ferramenta muito completa e extremamente útil para a gestão de domínios em .NZ.

DDoS .UG - Roy Arens, ICANN

Roy Arens, investigador sénior do ICANN e ex-colaborador do *Registry Nominet* (ccTLD .UK), apresentou dados interessantes que confirmam a expressão «Uma vez na Internet, para sempre na Internet», muitas vezes utilizada no âmbito dos dados pessoais, difíceis ou impossíveis de eliminar totalmente na Internet.

O servidor "ns.icann.org" com endereçamento IP 199.4.138.53 e 2001:500:89::53 , é há vários anos um dos servidores secundários para domínios do ICANN, como "icann.org" e "iana.org" entre outros. Através da análise do tráfego DNS neste servidor, verificou-se que 59% das consultas DNS são para o domínio "ip6.int", registado em 2001 e descontinuado em 2005, ou seja, um domínio que não existe há mais de 10 anos. Estes dados estão em linha com a análise que *Geoff Huston* da APNIC também já apresentou anteriormente noutras reuniões.

Em suma, este e os restantes dados analisados permitem concluir que o legado DNS do passado jamais desaparece, mesmo que os servidores de nomes de um domínio falhem, e até mesmo que o domínio não exista. Ainda, uma simples *botnet* (sistemas interligados para fins maliciosos), pode muito facilmente suprimir um domínio de topo com poucos recursos, como é o caso de muitos ccTLD's de pequena dimensão em Africa, mas não só. Numa expressão apenas: "*The Internet Never Forgets*".

Luminous - Norm Ritchie, SDF

Norm Ritchie, Chairman da Secure Domain Foundation (SDF) organização Canadiana sem fins lucrativos, fundada em 2014 com a missão de fortalecer a comunidade Internet no combate ao cibercrime, apresentou a plataforma *Luminous Intelligence*. Trata-se de uma solução que processa elevadas quantidades de indicadores resultantes de atividade maliciosa e cruza com informação do serviço *Whois*, para disponibilizar em tempo real, análises de reputação da informação DNS.

What3Words - Gary Gale, W3W

Gary Gale, CTO da iniciativa *What3Words* (w3w) apresentou o projeto com o mesmo nome. Ao contrário do que se possa pensar, um endereço postal não é para todos. Atualmente 75% do Mundo utiliza um sistema de endereçamento postal, inadequado, fraco ou inexistente. Mais de 4 biliões de pessoas não têm um endereço ou uma morada. Em países desenvolvidos como o Reino Unido, 0.5% das entregas postais falham devido a problemas de endereçamento, isto representa mais de 4,5 milhões de entregas sem sucesso por ano. Os problemas resultantes dos atuais sistemas de endereçamento são inúmeros, tanto em países desenvolvidos, como em países em desenvolvimento, e resultam em custos verdadeiramente elevados para estas comunidades.

O projeto *What3Words* divide todo o mundo em 57 triliões de secções de 3 por 3 metros, e a cada secção atribui um conjunto único de 3 palavras. É um conceito muito simples, e ao mesmo tempo muito eficaz.

Esquema de funcionamento do projeto *What3Words*

Este projeto foi apresentado na sessão *Tech Day* do ICANN por sugestão da organização do *Tech Day*. A semelhança do serviço DNS, tira proveito da capacidade humana para memorizar palavras em detrimento de números, sendo esse o principal motivo para se sobrepor ao atual sistema de geolocalização GPS. A principal questão identificada pela audiência presente, foi a possibilidade de gerar confusão com alguns domínios (sobretudo, novos gTLD's), por exemplo "mail.office.paris". Pode consultar mais informação acerca desta iniciativa em http://what3words.com/.

A sessão de *Workshop DNSSEC* da 56ª reunião do ICANN, ocorreu durante a tarde do passado dia 27-06-2016. Tal como sucedeu na sessão *TechDay*, esta sessão teve uma duração mais pequena do que o habitual devido ao novo formato das reuniões do ICANN. A próxima reunião do ICANN no final do ano deverá voltar ao formato normal, ou seja o *Workshop DNSSEC* terá uma agenda de um dia inteiro.
O comité do programa desta sessão tentou reunir conteúdos relacionados com os últimos desenvolvimentos relacionados com DNSSEC como é habitual, também projetos que optam por ativar ou não, o protocolo DNSSEC por omissão, e por último projetos/iniciativas relacionadas com algoritmos de encriptação utilizados no DNSSEC. Os temas apresentados foram os seguintes:

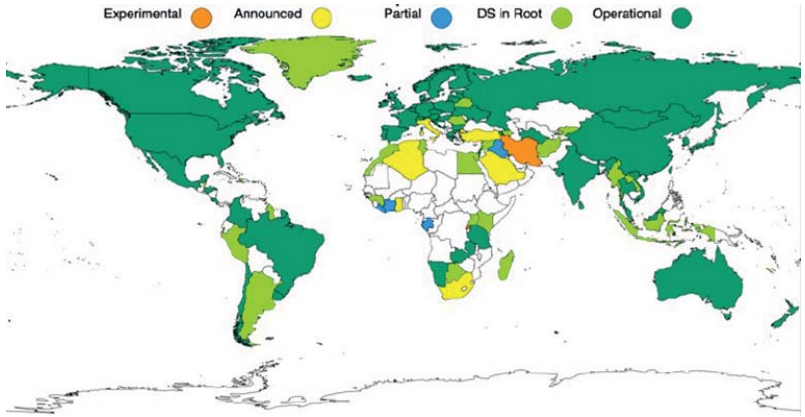
DNSSEC Workshop Introduction, Program, Deployment Around the World - Dan York, ISOC

Dan York da Internet Society (ISOC), fez a habitual introdução do workshop com a apresentação dos últimos dados relativos à implementação DNSSEC em termos globais.

Conforme se pode verificar na ilustração seguinte, a maioria dos domínios de topo (*ccTLD's*) já se encontram assinados com DNSSEC, à exceção dos ccTLD's em algumas regiões de Africa, Ásia Pacífico e América Latina, onde ainda existem trabalhos por fazer nesta área.

Desde da última reunião do ICANN em Marraquexe, houve desenvolvimentos em DNSSEC nos seguintes ccTLD's: .MA (Marrocos), .MG (Madagáscar) , .RO (Roménia), .SY (Síria) e .السعودية , (*Internationalized country code Top-Level Domain* ou ccTLD IDN do Reino da Arabia Saudita, neste caso não é a conversão direta de Arabia Saudita, mas sim o nome em língua árabe deste país).

Implementação DNSSEC em termos globais



Dos 1.363 domínios de topo (gTDL's e ccTLD's) na Internet à data de 23 de junho, 1.199 (88%) estão assinados com DNSSEC. Note-se que, por imposição do ICANN aplicável aos novos gTLD's, estes têm obrigatoriamente de estar assinados com DNSSEC desde do momento em que são criados.

Em termos de ccTLD's com a maior número de domínios assinados com DNSSEC, temos o .NL (Holanda) que lidera com 2.500.091 (44,5%), seguido do .BR (Brasil) com 918.637 (23,7%), e em terceiro o .CZ (República Checa) com 489.405 (63,4%) domínios assinados com DNSSEC. Em .PT há atualmente 13.534 (5%) domínios assinados com DNSSEC, um número pequeno comparado com os exemplos referidos, mas ao mesmo tempo já significativo tendo em consideração o panorama restantes ccTLD's.

Já nos gTLD's, o .COM lidera com 585.325 (0,46%), mas o destaque vai para o novo domínio de topo .OVH registado em julho de 2014 com 21.737 (44%) domínios com DNSSEC. Ainda, uma referência para os novos gTLD's .BANK e .INSURANCE, em que, como referido, por imposição contratual todos os subdomínios são obrigatoriamente assinados com DNSSEC.
Estes e outros dados, podem ser encontrados online em:

https://rick.eng.br/dnssecstat/,
http://stats.research.icann.org/dns/tld_report/,
https://ntldstats.com/dnssec.

Por último, uma referência à iniciativa *Global Commission on Internet Governance* (GCIG)(https://www.cigionline.org/activity/global-commission-internet-governance), projeto iniciado em 2014, liderado por Carl Bildt, ex-Primeiro Ministro e Ministro dos Negócios Estrangeiros da Suécia, e composto por 29 personalidades com currículos reconhecidos na área da governação da Internet. Esta iniciativa publicou no passado dia 21 de junho, o documento "*One Internet*" (http://ourinternet.org), que reúne vários pareces, diretrizes e recomendações em distintas áreas da governação da Internet, entre as quais, destacamos a seguinte recomendação, em linha com a estratégia que o DNS.PT tem vindo a adotar desde 2010, e que vem intensificar os esforços para a padronização do DNSSEC. ".

Recomendação para implementação DNSSEC

Recommendation

DNSSEC offers significant improvements to the current security of the DNS. Even though DNSSEC is currently being deployed, it is not happening quickly enough. Accelerating its adoption should be considered a high priority by DNS and network operators. It is essential that the Internet technical community's ongoing promotion efforts continue to support operators with the deployment of DNSSEC through the promotion of capacity-building programs, best practices and guidelines.

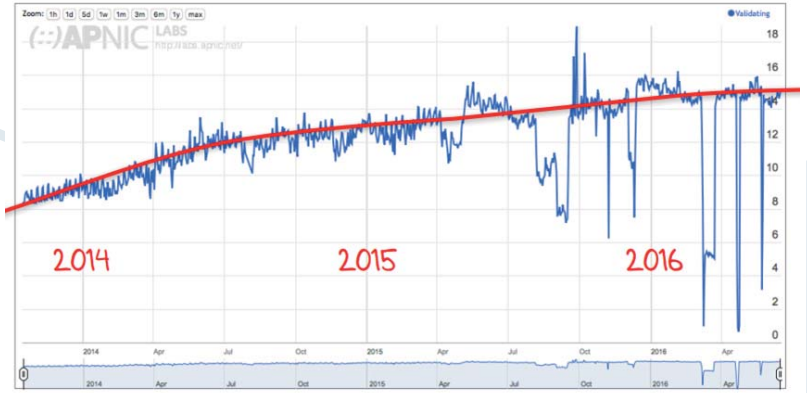
A versão integral do documento "One Internet" está disponível online em:
https://www.cigionline.org/sites/default/files/gcig_final_report_-_with_cover.pdf

A Quick Review of DNSSEC Validation in Today's Internet - Geoff Huston, APNIC

Geoff Huston, da APNIC, a entidade responsável pela gestão do espaço de endereçamento IP na região da Ásia e Pacífico, equivalente ao RIPE NCC para a Europa, apresentou os mais recentes resultados da sua análise sobre a taxa de penetração de DNSSEC na Internet, mais especificamente a capacidade de validação DNSSEC, pelos utilizadores da Internet.

Conforme se pode observar na ilustração seguinte, atualmente cerca de 15% do tráfego DNS global é devidamente validado com DNSSEC. Verifica-se ainda uma evolução positiva nos últimos 3 anos. Em Portugal esta taxa está situada em 8,90%. Estes dados estão disponíveis *online* com maior detalhe em:
http://stats.labs.apnic.net/dnssec.

Evolução global da validação DNSSEC



É importante referir que estes números são frequentemente influenciados pela utilização do serviço de resolução DNS do *Google* criado em finais de 2009, conhecido por *Google Public DNS* (PDNS). Este serviço, valida as consultas DNS com DNSSEC desde de janeiro de 2013, e é responsável pela resolução de um elevado número de consultas DNS por dia, cada vez maior.

Em Portugal, apesar de todos os esforços já realizados, nomeadamente a assinatura do .PT em janeiro de 2010, as inúmeras iniciativas realizadas desde então, com grande destaque para as sessões de *worshops* teórico/práticos de DNSSEC ainda é necessário que os *resolvers* DNS nacionais, procedam à validação DNSSEC do tráfego DNS nacional, para que o DNSSEC cumpra verdadeiramente os seus objetivos, tornando a Internet mais segura.

As datas dos Workshops DNSSEC do DNS.PT por realizar, são periodicamente publicadas na nossa página do facebook em https://www.facebook.com/dns.pt/app/206429986046631

Lying Makes Negative Answers Cheaper
Dani Grant, CloudFlare

Dani Grant da *CloudFlare*, empresa norte americana que comercializa serviços de *Global Content Delivery Network (CDN)*, apresentou a metodologia escolhida para otimizar as respostas DNS que resultam em *NXDOMAIN* (domínio não existe) e *NODATA* (domínio existe, mas o tipo de dados solicitado não).

De acordo com o RFC 4033, o protocolo DNSSEC garante essencialmente, a autenticação da origem, e a integridade dos dados. Adicionalmente garante ainda a não existência de um domínio. No entanto, o processo para provar a não existência de domínios dá origem a respostas DNS com um tamanho muito grande. Veja-se por exemplo, o caso do domínio "*bogus.ietf.org*" que não existe, sem DNSSEC a resposta tem 96 bytes, com DNSSEC tem 1.095 bytes, ambas para responder "*NXDOMAIN*". Adicionalmente, o serviço DNS é ineficiente quando tem de responder a consultas em que o domínio existe, mas o tipo de dados pedido não existe, ou seja uma resposta do tipo "*NODATA*".

Dado que estas situações representam um custo de performance na resolução DNS, a *CloudFlare* optou por criar e implementar duas soluções a que chama de "*Black Lies*" e "*DNS Shotgun*". A primeira aplica-se a respostas do tipo "*NXDOMAIN*", é baseada na solução "*NSEC3 White Lies*", referida no RFC 7129, mas com algumas alterações. A segunda solução é uma alteração na forma como o serviço DNS dá a resposta. A *CloudFlare* afirma que ambas soluções cumprem as especificações padrão do IETF.

DNSSEC Challenges
Ari-Matti Husa, FICORA

Ari-Matti Husa colaborador do *Registry FICORA*, apresentou alguns dados do .FI já anteriormente mencionados por *Juhani Juselius*. De destacar no entanto, que o.FI foi assinado com DNSSEC em 2010, mas ao contrário do que sucede nos países vizinhos (Suécia e Noruega), o número de domínios assinados é ainda muito baixo, aproximadamente 329 domínios (0,1%) e não existe aparentemente uma estratégia bem definida pelo .FI para mudar este cenário.

DNSSEC Deployment Challenges
Geoff Huston, APNIC

Geoff Huston de novo, sugere que a circunstância para o DNSSEC ainda não ter sido amplamente adotado está relacionado com o facto de existir um espaço entre o cliente e o *resolver*, em que a segurança do serviço DNS não é garantida pelo DNSSEC. *Geoff* sugere então, que a segurança do serviço DNS tem de ser garantida na componente aplicacional do lado do cliente, providenciando assim uma solução verdadeiramente *end-to-end*. Uma referência direta aos trabalhos (*getdns API*) de *Paul Hoffman*, publicados em abril de 2013 durante a reunião 86ª do IETF em Orlando (USA).

Key Signing Key Rollover and ZSK Length Increase
Matt Larson, ICANN e Duane Wessels, Verisign

Matt Larson, vice-presidente da área de investigação do ICANN e *Duane Wessels*, investigador sénior da *Verisign*, fizeram uma apresentação conjunta, relativa às chaves DNSSEC utilizadas na assinatura da zona raiz do DNS, gerida pela IANA.

Parâmetros atuais das chaves DNSSEC da zona raiz da Internet

Parameter	KSK	ZSK
Algorithm	8	8
Size	2048-bits	1024-bits
Rolled	(not yet*)	quarterly
Re-sign period	10 days	12 hours
Signature validity	15 days	10 days
Signs	DNSKEYs	everything else

Duane Wessels falou do processo de alteração do tamanho da chave *Zone Signing Key (ZSK)* da zona raiz, que irá duplicar, ou seja dos atuais 1024 bits para 2028 bits.

A calendarização dos momentos mais importantes destes trabalhos é a seguinte:

- 20 de setembro, publicação antecipada da nova chave ZSK com 2048-bits;
- 01 de outubro, a zona raiz é assinada com a nova chave ZSK de 2048-bits;
- Meados ou finais de outubro, a atual chave ZSK de 1024-bits, é removida;

Está previsto um processo para reverter estes trabalhos, caso seja necessário. Uma consequência da alteração do tamanho da chave ZSK é o aumento das respostas DNS, o que levou à realização de uma bateria exaustiva de testes, os resultados podem ser consultados online em:
http://keysizetest.verisignlabs.com/.

Matt Larson falou do processo de substituição da chave *Key Signing Key (KSK)* da zona raiz, mais conhecido por "*Root Key Rollover*", cujos planos serão publicados muito brevemente, dentro de alguns dias pelo ICANN. Podemos no entanto avançar as seguintes etapas:

- novembro de 2016, geração da nova chave KSK da zona raiz;
- fevereiro de 2017, a nova chave KSK ficará totalmente operacional.

Ainda, durante este processo estão previstas 3 alterações na zona raiz:

- julho de 2017, a nova KSK será publicada na zona raiz;
- outubro de 2017, a nova KSK será utilizada no processo de assinatura DNSSEC da zona raiz;
- janeiro de 2018, a atual KSK será revocada.

O plano prevê ainda a possibilidade de retrocesso, em caso de necessidade, mas só até a revocação da atual chave.

Esta alteração vai requerer que todos os *resolvers* DNS na *Internet*, atualizem a chave KSK da zona raiz, e aqui há duas possibilidades, utilizar os mecanismos *Automated Updates of DNSSEC Trust Anchors*, especificado no RFC 5011, ou proceder de forma manual à adição da nova chave KSK, até outubro de 2017, e remoção da atual KSK numa data posterior, isto se as datas atuais se mantiverem, conforme planeado.

Em suma, trata-se de um processo sobejamente discutido e estudado, que irá ser executado por fases bem delineadas, e de forma muito controlada, dada a criticidade do mesmo.

DNSSEC Encryption Algorithms
Ondrej Surý, CZNIC e Dan York, ISOC

Dan York de novo, falou da agilidade do processo de adoção de novos algoritmos de encriptação utilizados no DNSSEC, cuja lista é extensa, e está disponível *online* em http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml.

A comunidade de especialistas técnicos em DNSSEC está atenta a novos algoritmos, porque estes representam um conjunto de vantagens, nomeadamente, a rapidez dos processos criptográficos, chaves e assinaturas mais pequenas, e sobretudo resultam numa melhor criptografia.

No entanto, o processo de implementação de novos algoritmos é por norma muito demorado, pelo que é preciso agilizar este processo, nomeadamente através da elaboração de documentação e a consciencialização de utilizadores específicos, para a importância de suportar a adoção de novos algoritmos criptográficos, nomeadamente no desenvolvimento e atualização de plataformas de DNSSEC dos *Registries*, *Registrars* e as demais entidades que participam em processos que operam com DNSSEC.

Até ao momento, já foram realizadas várias sessões nas principais reuniões da comunidade de especialistas da Internet, como o ICANN, o DNS-OARC, o IETF e o RIPE. Também, em março deste ano foi publicado o *draft* com o título "*Observations on Deploying New DNSSEC Cryptographic Algorithms*" disponível *online* em https://datatracker.ietf.org/doc/draft-york-dnsop-deploying-dnssec-crypto-algs/.

dns.pt
dnssec.pt
facebook.com/dns.pt
pt.linkedin.com/in/dnspt

ASSOCIAÇÃO dns.pt

Produção: julho 2016
Grafismo: dns.pt