

Tópicos sobre DNS

Daniel Fink daniel.fink@icann.org

IX (PTT) Fórum Regional – Teresina PI
Junho 2018



O que é a ICANN?

- ▮ Missão
- ▮ Estrutura
- ▮ Modelo Multisetorial
- ▮ O grupo dos provedores na ICANN
- ▮ IANA / PTI
- ▮ Partes contratadas

Aspectos técnicos

- ▮ Processo de resolução
- ▮ Servidores Raiz
- ▮ L-root

Anúncios importantes

- ▮ DNSSEC
- ▮ KSK Rollover
- ▮ Universal acceptance
- ▮ Referências

O que é a ICANN?

Corporação
da Internet
para Designação
de Nomes
e Números

Nomes & Números

ICANN.org

=

192.0.32.7



Missão da ICANN

Especificamente, a ICANN:

- ✓ Coordena a alocação e a atribuição de **nomes na zona raiz do Sistema de Nomes de Domínio (DNS)**
- ✓ Coordena o desenvolvimento e a implementação de **políticas relacionadas a registros de nomes de domínio de segundo nível em Domínios Genéricos de Primeiro Nível (gTLDs)**
- ✓ Promove a coordenação da operação e a **evolução do sistema de servidor de nomes da raiz do DNS**
- ✓ Coordena a alocação e a atribuição no nível mais alto de **números de Protocolo da Internet (IP) e números de Sistemas Autônomos**
- ✓ Colabora com outras entidades, conforme apropriado, para **fornecer os registros necessários para o funcionamento da Internet**, de acordo com as especificações das organizações de desenvolvimento de padrões de protocolo da Internet

A missão da Corporação da Internet para Atribuição de Nomes e Números (ICANN) é **garantir a operação estável e segura dos sistemas de identificadores exclusivos da Internet**

Para mais informações,



visite:
www.icann.org

Compromissos e valores essenciais

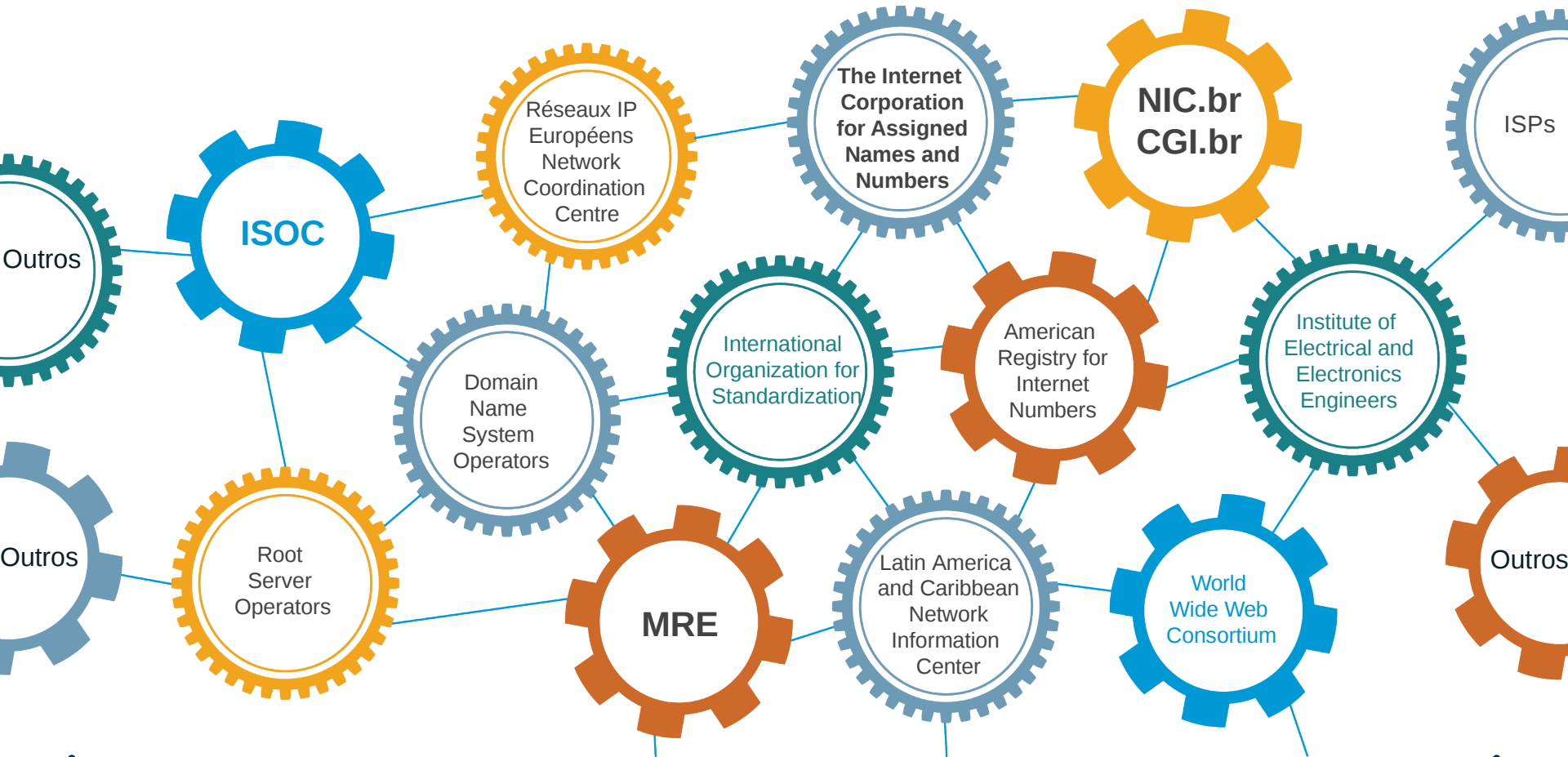
Ao desempenhar sua missão, a ICANN atuará de forma a cumprir e refletir seus compromissos e a respeitar seus valores essenciais

Esses compromissos e valores essenciais incluem:

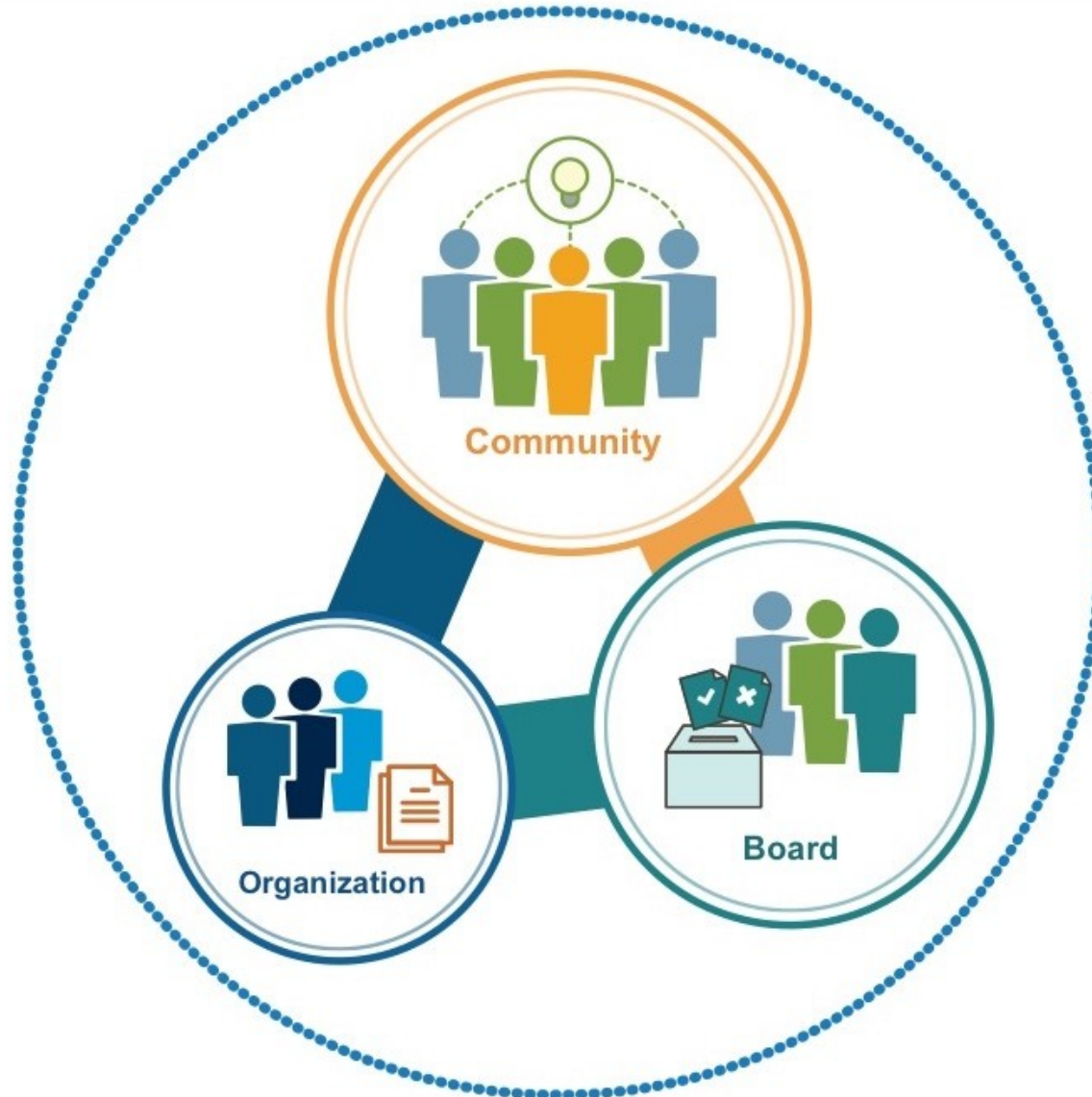
- Preservar e melhorar a **estabilidade**, a **segurança**, a **resiliência** e a **abertura** do DNS e da Internet
- Utilizar processos de múltiplas partes interessadas **abertos, transparentes e ascendentes** para o desenvolvimento de políticas que sejam liderados pelo setor privado
- Atuar com **eficiência** e **excelência**, demonstrando integridade tributária e responsabilidade

Nossos parceiros

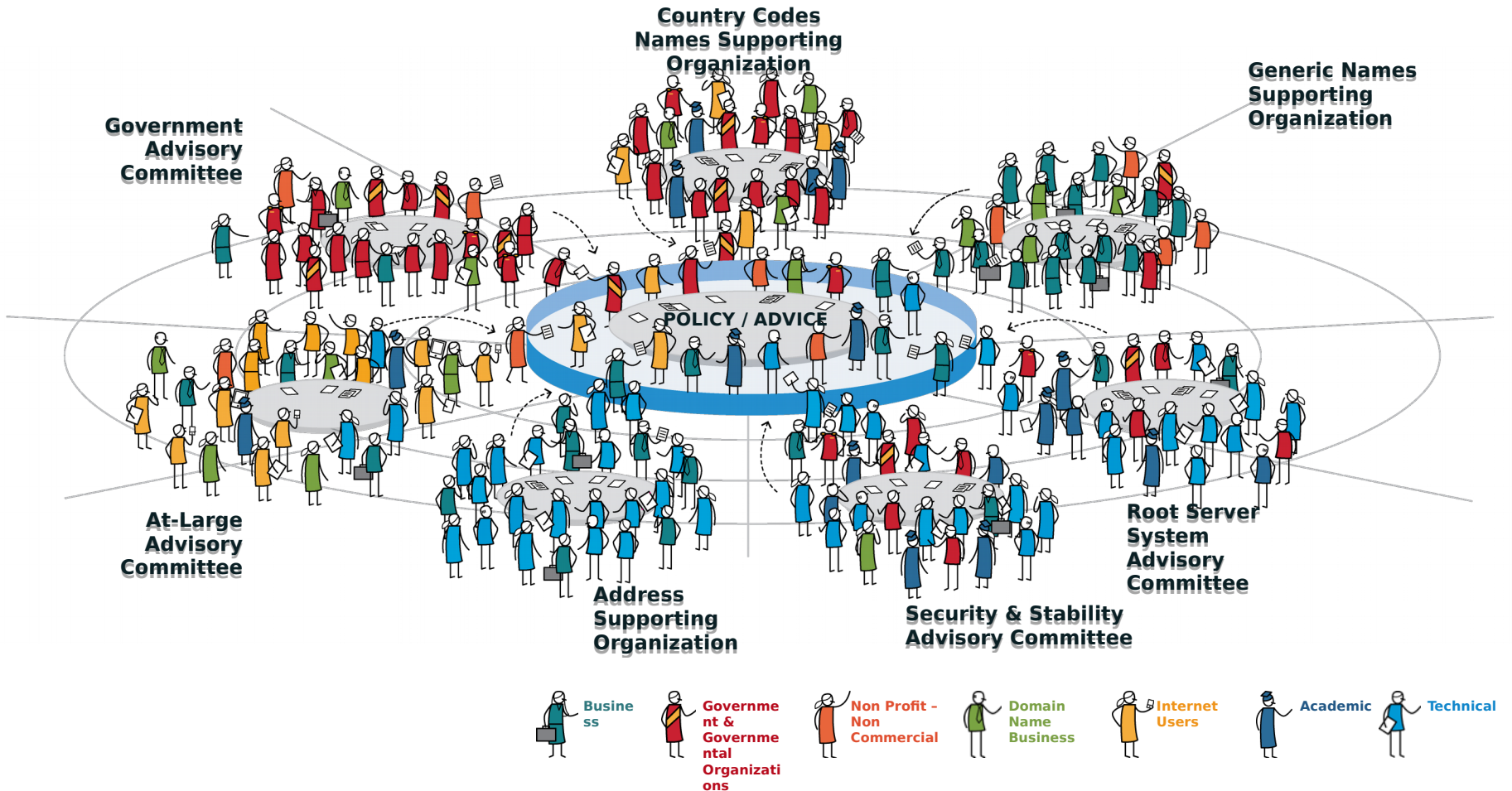
Em coordenação com nossos parceiros, ajudamos a fazer a Internet funcionar.



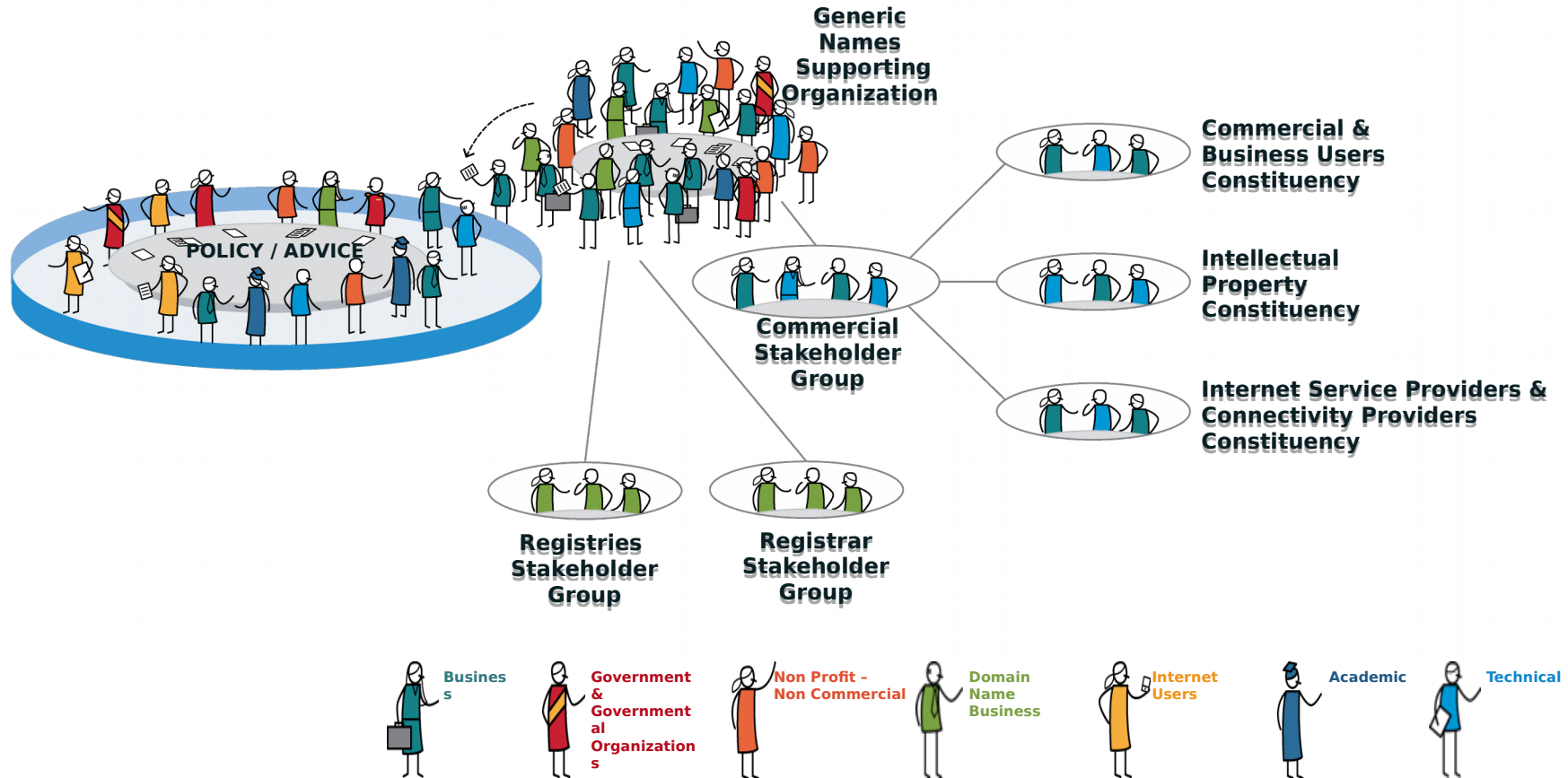
Estrutura da ICANN



Comunidade Multissetorial ICANN



Setor Privado



ICANN | ISPCP

Internet Service Providers & Connectivity Providers

Representa o setor de conectividade, contribui nas diversas discussões técnicas e macropolíticas:

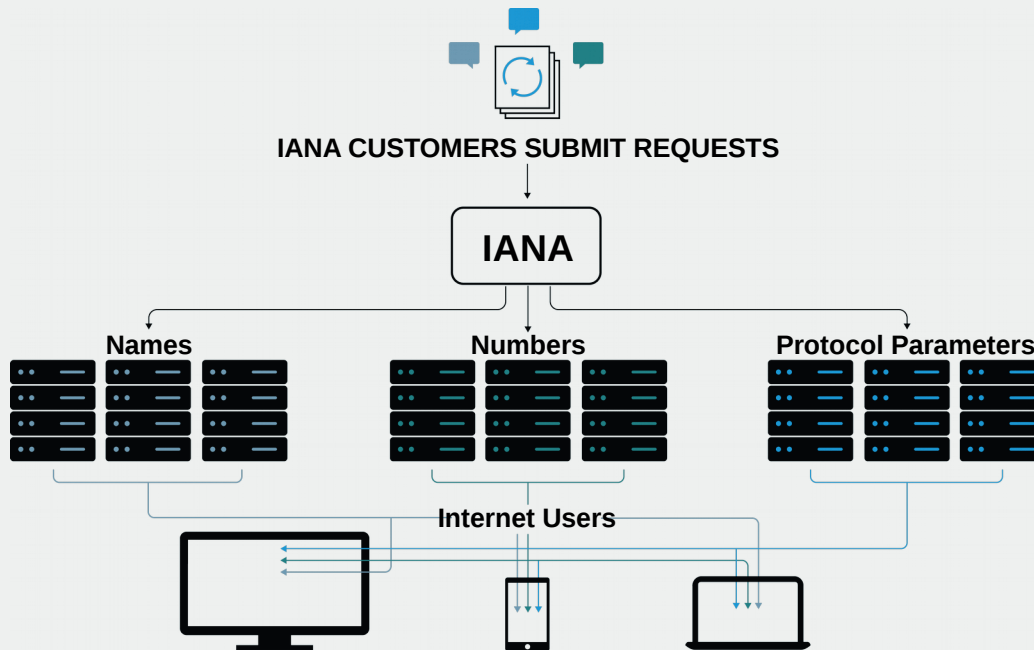
- Impacto do lançamento de novos nomes de domínio genéricos
- Universal Acceptance
- Impactos dos novos gTLD's

Se você é um provedor de Internet, participe da ISPCP na ICANN. Não há custos, simplesmente cadastre-se e receberá todas as novidades e oportunidades para participar nas atividades do grupo. Ademais, você poderá antecipar-se às oportunidades de negócios quando surgirem.

Visite: <http://www.ispcp.info>

IANA - Autoridade para Atribuição de Números da Internet

Supervisiona a atribuição global dos números na Internet - entre os quais estão os números das portas, os endereços IP, sistemas autónomos, servidores-raiz de números de domínio DNS e outros recursos relativos aos protocolos de Internet.

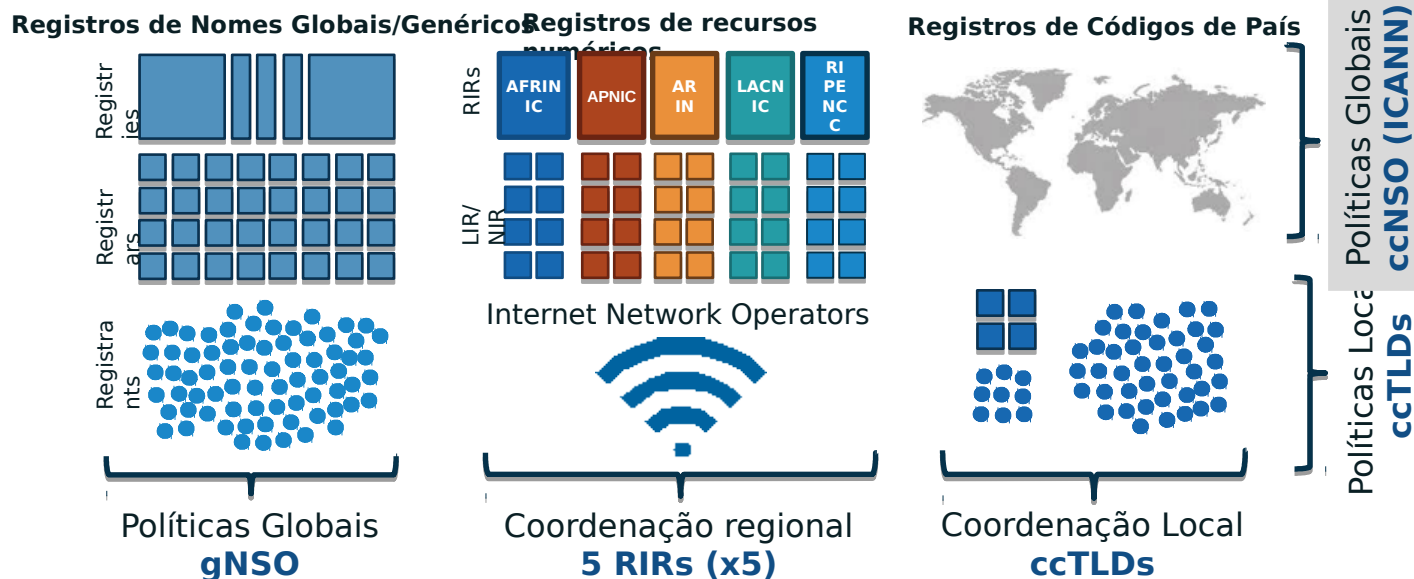


Essas funções incluem:

- A coordenação da atribuição de parâmetros técnicos de protocolo da Internet.
- A administração de certas responsabilidades associadas ao gerenciamento de zona raiz do DNS da Internet.
- A alocação de endereços IP da Internet.

A ICANN foi criada para executar as funções da IANA e fez isso de acordo com um contrato sem custo com o Departamento de Comércio por mais de 15 anos.

Framework de Desenvolvimento de Políticas de Identificadores



- Altamente recomendável acompanhar e participar:

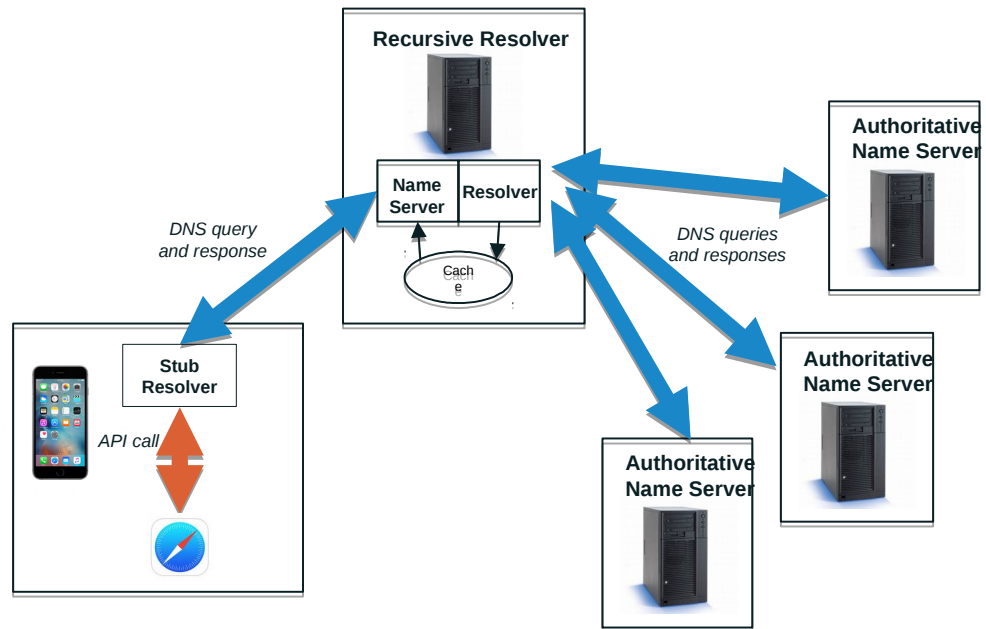


Aspectos técnicos

Estrutura do DNS

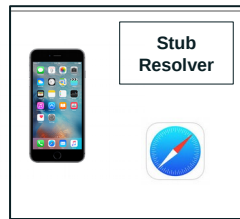
- DNS é uma base de dados distribuída
 - Dados são mantidos localmente, mas disponíveis globalmente
- **Resolvedores** enviam consultas
- **Servidores de Nomes** enviam respostas
- Otimizações:
 - Caching para melhorar desempenho
 - Replicação para prover redundância e distribuição de carga

Componentes do DNS



O telefone é configurado para enviar consultas para o resolvedor recursivo com IP 4.2.2.2

Recursive Resolver
4.2.2.2



*4.2.2.2 is a recursive resolver
run by Level 3 Communications*

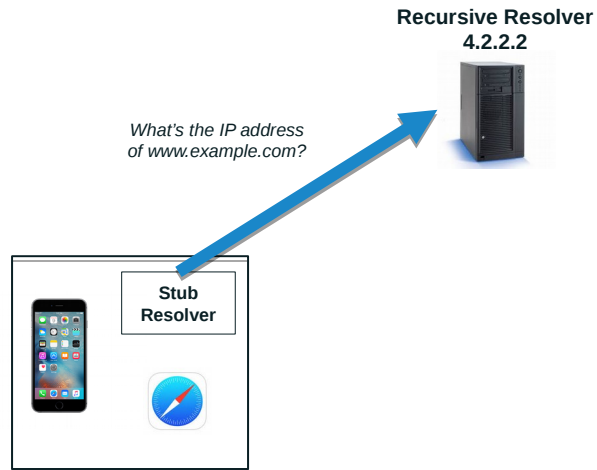
O usuário digita www.example.com no Safari do seu telefone. Safari inicia função para resolver nome.

Recursive Resolver
4.2.2.2



Processo de resolução

O telefone envia a consulta
www.example.com, IN, A para o 4.2.2.2



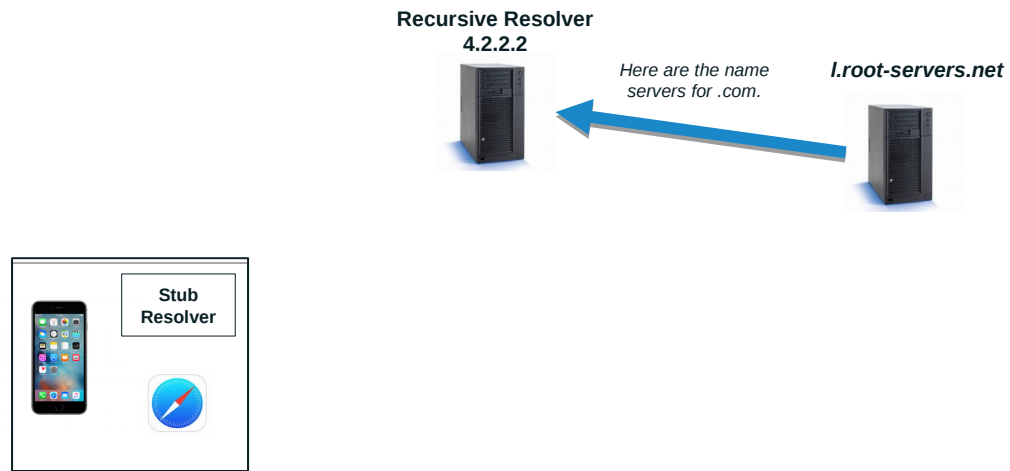
Processo de resolução

Como o cache está vazio, o servidor recursivo pergunta para o servidor raiz



Processo de resolução

O servidor raiz responde apontando os servidores do .com



Processo de resolução

Servidor recursivo pergunta para o servidor .com



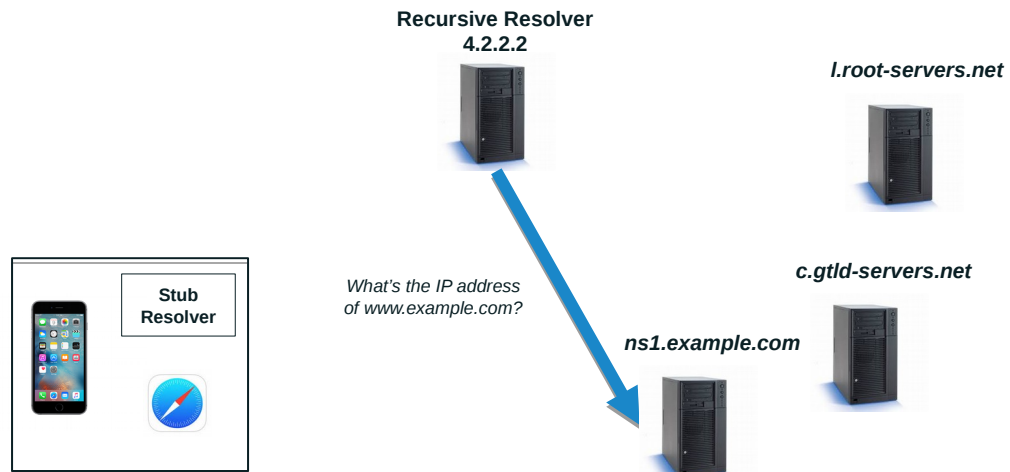
Processo de resolução

O servidor .com responde apontando o servidor de nomes para o example.com



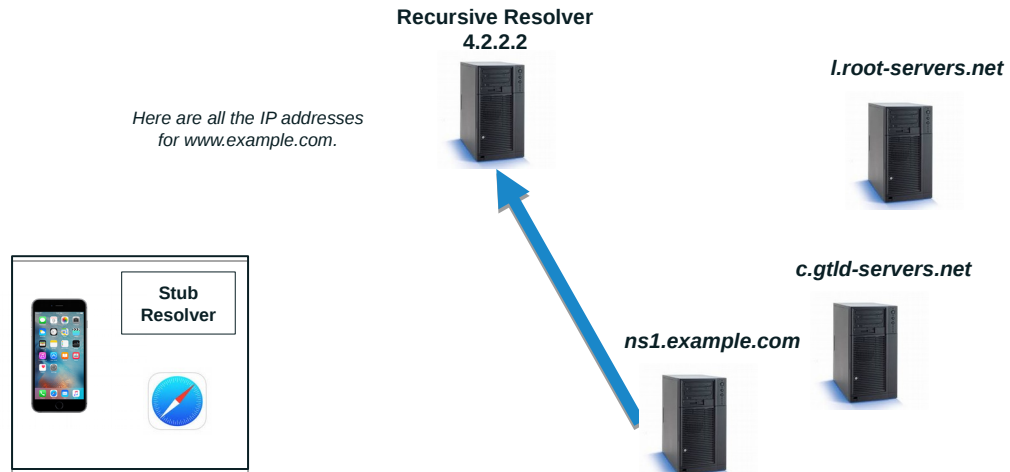
Processo de resolução

Servidor recursivo pergunta para o servidor do example.com



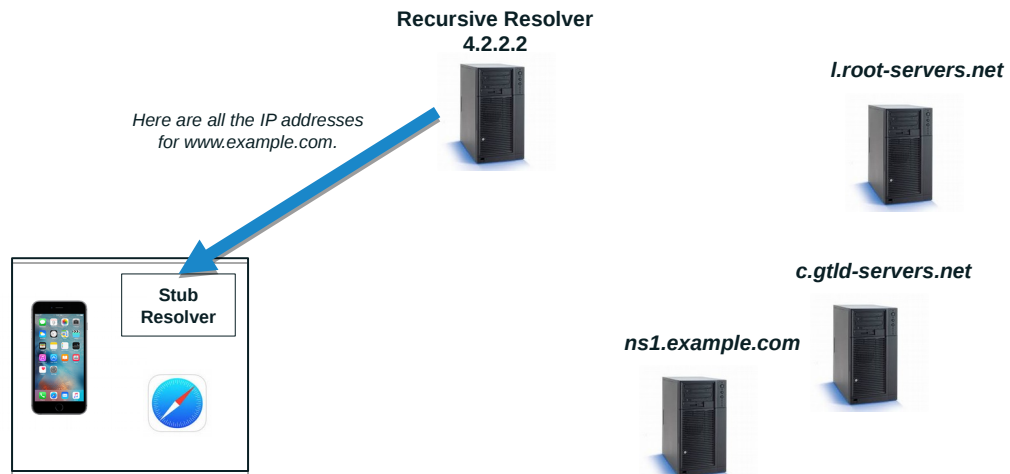
Processo de resolução

Servidor example.com responde a pergunta ao servidor recursivo



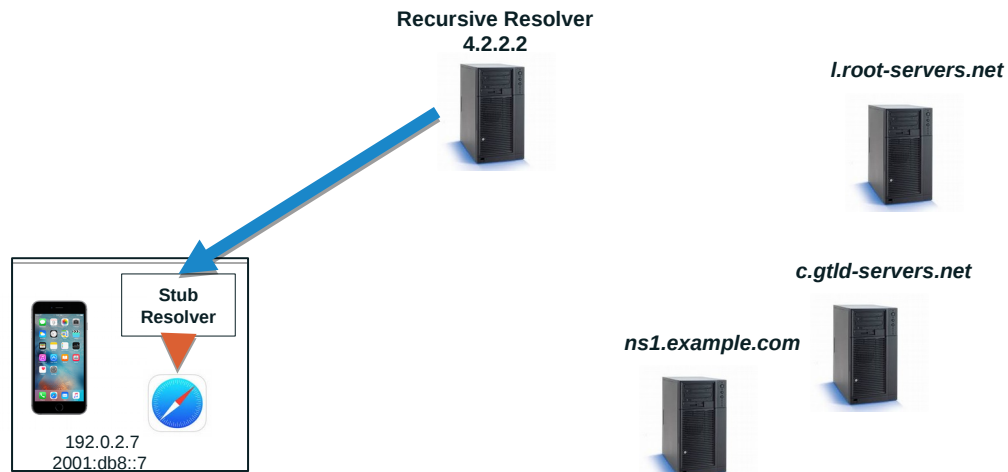
Processo de resolução

Servidor recursivo envia a resposta para o telefone



Processo de resolução

Sabendo o número IP, o Safari pode fazer a conexão com o website `www.example.com`.



- ▮ Caching acelera o processo de resolução
- ▮ Depois da consulta prévia, o servidor recursivo 4.2.2.2 sabe:
 - ▮ Nomes e endereços IP dos servidores *.com*
 - ▮ Nomes e endereços IP dos servidores *example.com*
 - ▮ Endereços IP do servidor *www.example.com*

Servidores Raiz

The Root Servers and Operators

- A** Verisign
- B** University of Southern California Information Sciences Institute
- C** Cogent Communications, Inc.
- D** University of Maryland
- E** United States National Aeronautics and Space Administration (NASA) Ames Research Center
- F** Information Systems Consortium (ISC)
- G** United States Department of Defense (US DoD)
Defense Information Systems Agency (DISA)
- H** United States Army (Aberdeen Proving Ground)
- I** Netnod Internet Exchange i Sverige
- J** Verisign
- K** Réseaux IP Européens Network Coordination Centre (RIPE NCC)
- L** Internet Corporation For Assigned Names and Numbers (ICANN)
- M** WIDE Project (Widely Integrated Distributed Environment)

news [see all news items](#)

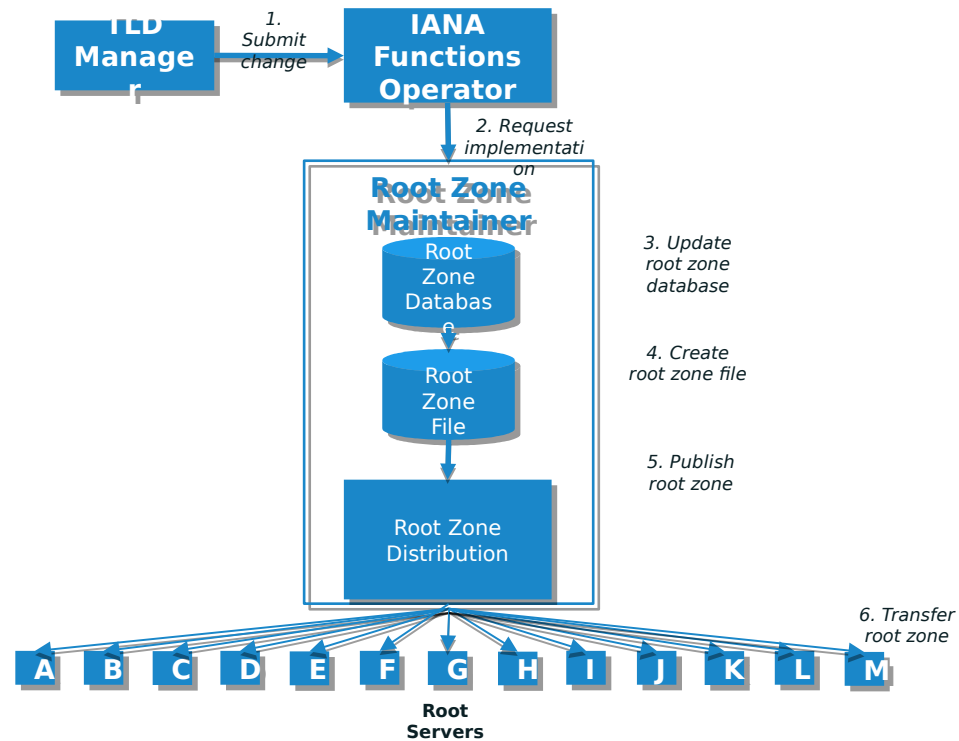
- 2017-09-19 [Statistics About DNS Root Name Service](#)
- 2017-08-10 [B-Root's IPv4 address to be renumbered on 2017-10-24](#)
- 2017-04-17 [B-Root Begins Anycast in May](#)

meeting agendas [see all agenda items](#)

- 2018-03-18 [IETF 101/London \(PDF\)](#)
- 2017-11-12 [IETF 100/Singapore \(PDF\)](#)
- 2017-07-16 [IETF 99/Prague \(PDF\)](#)
- 2017-03-26 [IETF 98/Chicago \(PDF\)](#)



Processo de mudanças na Zona Raiz



L-root

Qual o servidor raiz mais próximo?

```
$ dig @1.root-servers.net id.server ch txt
```

```
[DAFI-5572:~ daniel.fink$ dig @l.root-servers.net id.server ch txt
; <<>> DiG 9.8.3-P1 <<>> @l.root-servers.net id.server ch txt
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28845
;; flags: qr rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;id.server.                CH      TXT

;; ANSWER SECTION:
id.server.                0      CH      TXT      "gru01.l.root-servers.org"

;; Query time: 22 msec
;; SERVER: 199.7.83.42#53(199.7.83.42)
;; WHEN: Mon Mar 26 11:45:47 2018
;; MSG SIZE rcvd: 64
```

```
[DAFI-5572:~ daniel.fink$ dig @l.root-servers.net id.server ch txt
; <<>> DiG 9.8.3-P1 <<>> @l.root-servers.net id.server ch txt
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60716
;; flags: qr rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;id.server.                CH      TXT

;; ANSWER SECTION:
id.server.                0      CH      TXT      "iad54.l.root-servers.org"

;; Query time: 140 msec
;; SERVER: 199.7.83.42#53(199.7.83.42)
;; WHEN: Mon Mar 26 11:48:56 2018
;; MSG SIZE rcvd: 64
```

DNSSEC

Implementação

da nova Chave de Assinatura de
Chaves (KSK)

O que é DNSSEC?

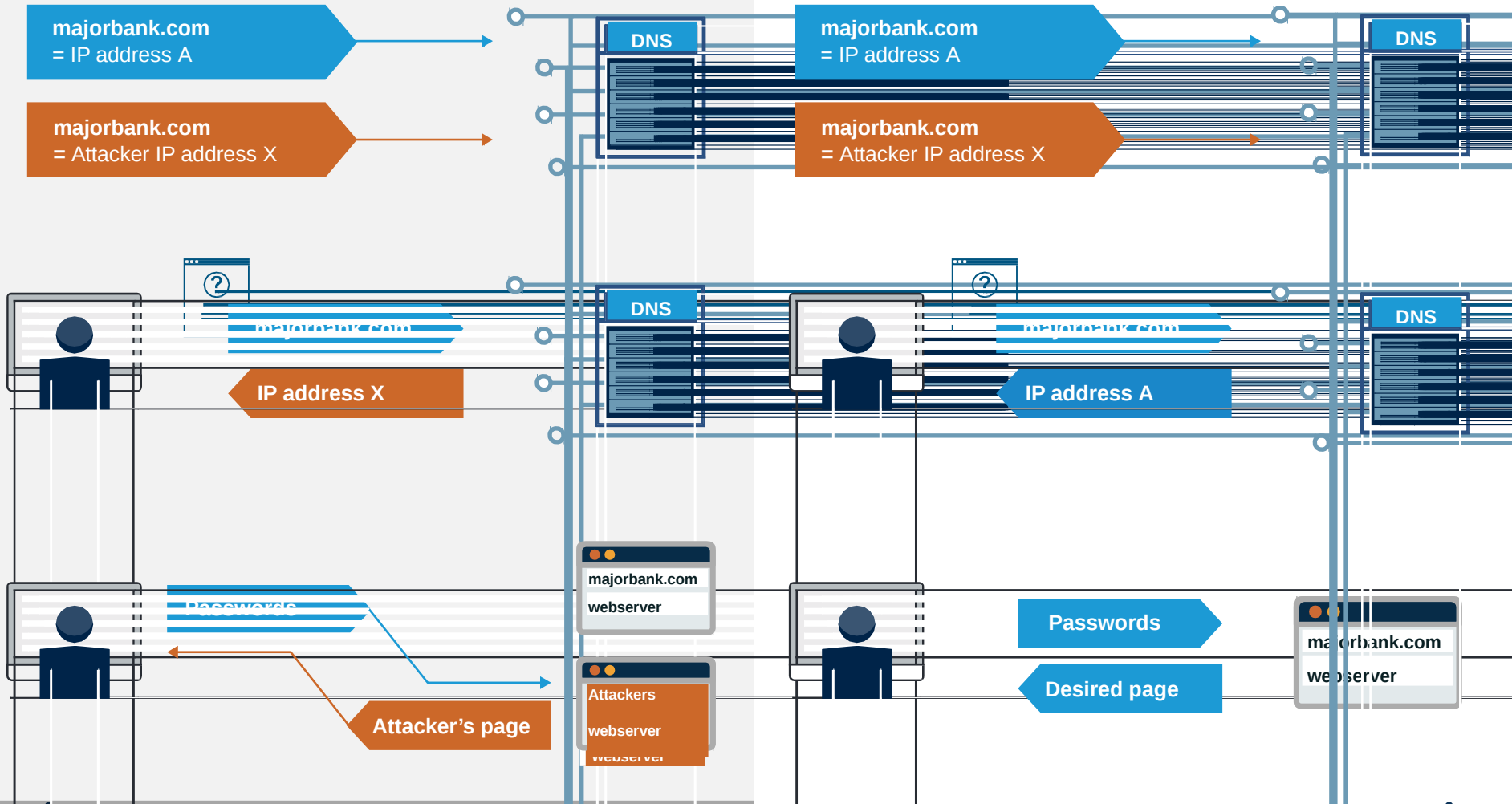


- ▮ DNSSEC = “**DNS Security Extensions**”
- ▮ É um protocolo que está sendo implantado atualmente para proteger o Sistema de Nomes de Domínio (DNS).
- ▮ O DNSSEC adiciona segurança ao DNS ao incorporar criptografia de chave pública na hierarquia do DNS, resultando em uma PKI (Public Key Infrastructure, infraestrutura de chave pública) única e aberta para nomes de domínio.
- ▮ Resultado de mais de uma década de desenvolvimento de padrões abertos

Como DNSSEC funciona?

Sem DNSSEC

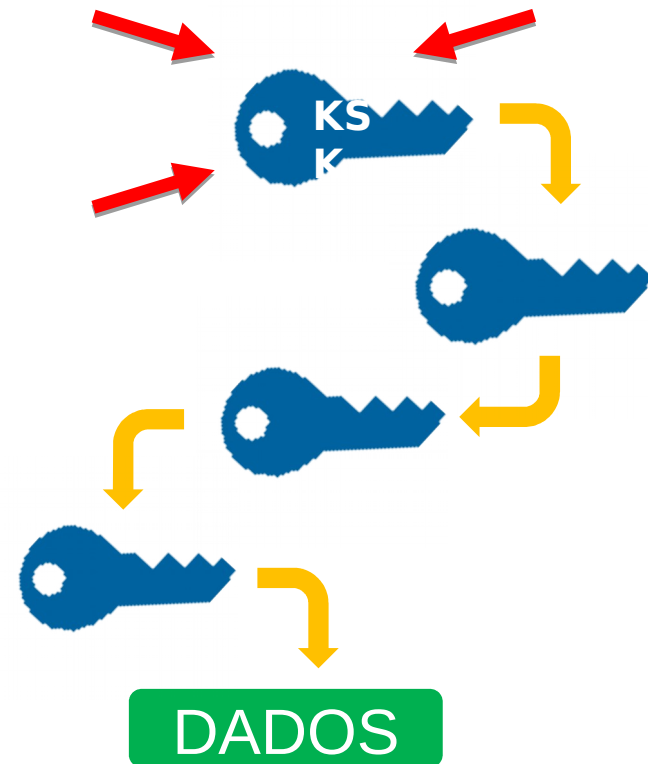
Com DNSSEC



Implementação da KSK: Uma Visão Geral

A ICANN está prestes a realizar a implementação da Chave de Assinatura de Chaves (KSK) das Extensões de Segurança do DNS (DNSSEC) da zona raiz

- A “**KSK**” (Chave de Assinatura de Chave) de DNSSEC da zona raiz é a principal chave criptográfica na hierarquia do DNSSEC
- A KSK é um par de chaves criptográficas públicas e privadas:
 - Parte pública: ponto inicial confiável para a validação de DNSSEC
 - Parte privada: assina a Chave de Assinatura de Zona (ZSK)
- Constrói uma “cadeia de confiança” de chaves e assinaturas sucessivas para validar a autenticidade de quaisquer dados assinados no DNSSEC



Por que a ICANN está fazendo a implementação da KSK?

- Porque não é bom que uma chave criptográfica continue sempre a mesma. As chaves criptográficas usadas nos dados DNS de assinatura de DNSSEC devem ser alteradas periodicamente
 - Garante que a infraestrutura tenha suporte para a alteração de chaves no caso de emergência
- Esse tipo de alteração nunca foi realizada antes no nível da raiz
 - Há uma única KSK de DNSSEC da zona raiz funcional e operacional desde 2010
- Porque é melhor fazer mudanças proativas durante a operação normal, quando as coisas estão funcionando bem, em vez de responder a emergências. A implementação da KSK precisa de uma coordenação ampla e cuidadosa para garantir que ela não interfira nas operações normais

DNSSEC

Quando será feita a implementação?

- ▮ A mudança ou "rolagem" da chave KSK estava programada para ocorrer em 11 de outubro de 2017, mas foi adiada porque alguns dados obtidos em setembro de 2017 mostraram que um número significativo de resolvedores usados por provedores de serviços de Internet (ISPs) e operadores de rede ainda não está pronto para a mudança de chave.
- ▮ Pode haver vários motivos pelos quais os operadores não têm o novo KSK instalado em seus sistemas: alguns podem não ter seu software de resolução configurado adequadamente.
- ▮ Depois de uma consulta preliminar com a comunidade, a ICANN publicou um plano para iniciar o processo de rolagem novamente. Esse plano foi aberto para comentários da comunidade em <https://www.icann.org/public-comments/ksk-rollover-restart-2018-02-01-en> .
- ▮ O plano pede que a ICANN implante o KSK raiz em **11 de outubro de 2018**, incentivando os ISPs e os operadores de rede a usar esse período adicional para garantir que seus sistemas estejam prontos para a substituição de chaves.

Quem será afetado?

Desenvolvedores
e distribuidores de
software do DNS

Integradores
de sistemas

Operadores de
rede

Operadores do
servidor raiz

Operadores do
servidor raiz

Usuários
finais
*(se nenhuma ação for
realizada pelos operadores
resolvedores)*



Se você ativou a validação de DNSSEC, é necessário atualizar seus sistemas com a nova KSK para garantir que os usuários tenham acesso à Internet sem problemas

- ▮ Atualmente, 25% dos usuários da Internet no mundo todo, ou **750 milhões de pessoas**, usam resolvers de validação de DNSSEC que poderão ser afetados pela implementação da KSK
- ▮ Se esses resolvers de validação não tiverem a nova chave quando a KSK for implementada, os usuários finais que dependem deles encontrarão erros e **não poderão acessar a Internet**

O que os operadores precisam fazer?



Verificar se o DNSSEC está ativado nos seus servidores



Verificar como a confiança é avaliada nas suas operações



Testar/verificar suas configurações



Inspecionar os arquivos de configuração para ver se eles (também) estão atualizados



Se a validação de DNSSEC está ativada ou planejada no seu sistema

- Tenha um plano para participar na implementação da KSK
- Conheça as datas, os sintomas e as soluções

Verifique se os seus sistemas estão prontos

A ICANN está oferecendo um **ambiente de teste** para os operadores ou qualquer parte interessada confirmarem se os seus sistemas dão conta do processo automático de atualização corretamente.

Verifique se os seus sistemas
estão prontos acessando:
go.icann.org/KSKtest

Automated Trust Anchor Update Testbed

The root zone Key Signing Key (KSK) is changing, or rolling, on 11 October 2017. Operators of recursive resolvers with DNSSEC validation enabled will need to ensure that their systems are updated with the new root zone KSK configured as a trust anchor before that date. If a recursive resolver supports RFC 5011, "Automated Updates of DNS Security (DNSSEC) Trust Anchors", and this feature is properly configured, the new KSK should automatically be installed as a trust anchor and DNSSEC validation should continue without problems.

If a validating resolver's implementation or configuration of the RFC 5011 automated trust anchor update protocol is incorrect for any reason, then its configuration might not be properly updated during the root zone KSK roll and resolution would fail after 11 October 2017.

This testbed allows operators of validating resolvers to test their implementation and confirm its ability to properly follow a KSK roll and update its trust anchor configuration.

This test tool assumes that you understand [the upcoming KSK change](#), and at least some about [RFC 5011](#).

Purpose of This Testbed

The test system described here allows the operator of a validating recursive resolver to test its support for the RFC 5011 automated trust anchor update protocol and therefore its readiness for the root zone KSK roll. The test operates in real time and should not affect the resolver's normal operation. The testbed works by starting a KSK roll in a new zone each week. These test zones are not used for any other purpose. For example, the current zone name is [2017-03-26.automated-ksk-test.research.icann.org](#). Because this zone is used only for the testbed and contains no names any



Se o seu software for compatível com atualizações automáticas das âncoras de confiança de DNSSEC (RFC 5011):

- A KSK será atualizada automaticamente no momento apropriado
- Você não precisará realizar nenhuma ação adicional
 - Os dispositivos off-line durante a implementação precisarão ser atualizados manualmente quando estiverem on-line após o término da implementação



Se o seu software não for compatível com atualizações automáticas das âncoras de confiança de DNSSEC (RFC 5011) ou não estiver configurado para usar esse recurso:

- O arquivo da âncora de confiança do software precisará ser atualizado manualmente
- A nova KSK de zona raiz está disponível aqui após março de 2017:

[http://data.iana.org/
root-anchors/](http://data.iana.org/root-anchors/)



- ▣ A tag chave da KSK-2017 é

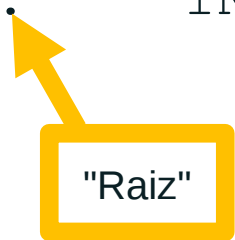
20326

- ▣ O registro de recurso do Signatário de Delegação (DS) da KSK-2017 é

IN DS 20326 8 2

E06D44B80B8F1D39A95C0B0D7C65D084

58E880409BBC683457104237C7F8EC8D



Observação: a formatação foi alterada para esta apresentação



▮ O registro de recurso de DNSKEY será:

. IN DNSKEY 257 3 8

AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3
+/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv
ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLRjyBxWezF
0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuV7pr+e
oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd
RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN
R1AkUTV74bU=

"Raiz"

To distinguish between the old root root key-signing key and the new one, the old root zone key-signing key will appear as:

```
AwEAAagAIK1VZrpC6Ia7gEzahOR+9W29euxhJhVVL0yQbSEW008gcCjFFVQUTf6v58fLjwBd0YI0Ezr  
AcQqBGCzh/RStIo08g0NfnfL2MTJRkxoX bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf  
S/Efucp2gaDX6RS6CXpoY68LsvPvjR0ZSwzz1apAzvN9dLzEheX7ICJBBtuA6G3LQpzW5h0A2hzCTMj  
JPJ8LbqF6dsV6DoBQzgul0sGIcGOYl70yQdXfZ57re1sQageu+ipAdTTJ25AsRTAoub80NGcLmqrAmR  
LKBP1dfwhYB4N7knNnulqxA+Uk1ihz0=
```

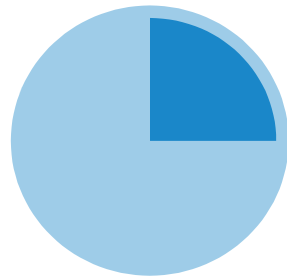
The new (current) root zone key-signing key will appear as:

```
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlExOL  
AJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3Eg  
VLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuV7pr+eoZG+SrDK6nWe  
L3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd RUfhHdY6+cn8HFRm+2hM8AnXGXws9555Kr  
UB5qihylGa8subX2Nn6UwNR1AkUTV74bU=
```

Aceitação Universal

Exercício

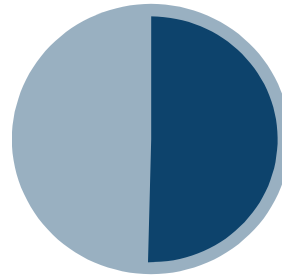
Qual destes gráficos mostra a fração de de sites que usam inglês como idioma primário?



25%

Inglês

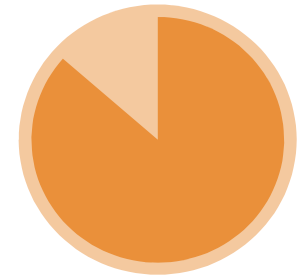
25% Inglês
75% Outros



50%

Inglês

50% Inglês
50% Outros



75%

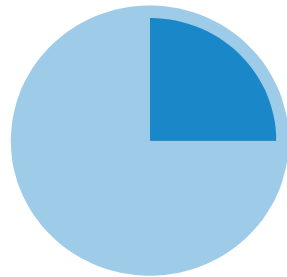
Inglês

75% Inglês
25% Outros

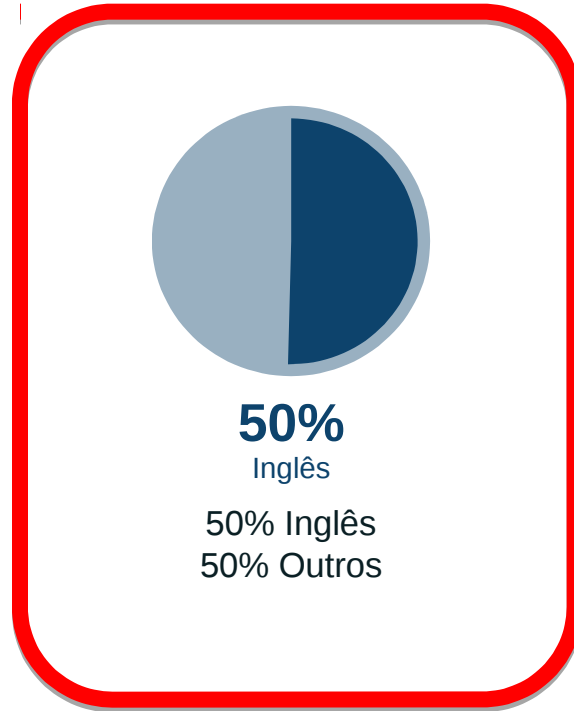
[/w3techs.com/technologies/history_overview/content_language/ms/y](http://w3techs.com/technologies/history_overview/content_language/ms/y)

Exercício

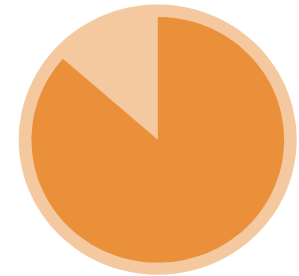
Qual destes gráficos mostra a fração de de sites que usam inglês como idioma primário?



25%
Inglês
25% Inglês
75% Outros



50%
Inglês
50% Inglês
50% Outros



75%
Inglês
75% Inglês
25% Outros



أحمد@سابقة.تونس



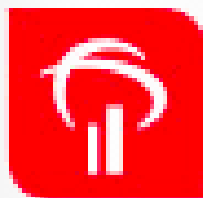


https://banco.bradesco/



ACESSE O INTERNET BANKING

Agência:



Bradesco

ABRA SUA CONTA

Pre
Co

Root Zone Database

The Root Zone Database represents the delegation details of top-level domains, including gTLDs such as .com, and country-code TLDs such as .uk. As the manager of the DNS root zone, we are responsible for coordinating these delegations in accordance with our [policies and procedures](#).

Much of this data is also available via the WHOIS protocol at whois.iana.org.

DOMAIN	TYPE	TLD MANAGER
.aaa	generic	American Automobile Association, Inc.
.aarp	generic	AARP
.abarth	generic	Fiat Chrysler Automobiles N.V.
.abb	generic	ABB Ltd
.abbott	generic	Abbott Laboratories, Inc.
.abbvie	generic	AbbVie Inc.
.abc	generic	Disney Enterprises, Inc.
.able	generic	Able Inc.
.abogado	generic	Top Level Domain Holdings Limited
.abudhabi	generic	Abu Dhabi Systems and Information Centre
.ac	country-code	Network Information Center (AC Domain Registry) c/o Cable and Wireless (Ascension Island)
.academy	generic	Binky Moon, LLC
.accenture	generic	Accenture plc
.accountant	generic	dot Accountant Limited
.accountants	generic	Binky Moon, LLC
.aco	generic	ACO Severin Ahlmann GmbH & Co. KG
.active	generic	Active Network, LLC

.测试	test	Internet Assigned Numbers Authority
.कॉम	generic	VeriSign Sarl
.परीक्षा	test	Internet Assigned Numbers Authority
.セール	generic	Amazon Registry Services, Inc.
.佛山	generic	Guangzhou YU Wei Information Technology Co., Ltd.
.ଭାରତ	country-code	National Internet eXchange of India
.慈善	generic	Excellent First Limited
.集团	generic	Eagle Horizon Limited
.在线	generic	TLD REGISTRY LIMITED
.한국	country-code	KISA (Korea Internet & Security Agency)
.ଭାରତ	country-code	National Internet eXchange of India
.大众汽车	generic	Volkswagen (China) Investment Co., Ltd.
.点看	generic	VeriSign Sarl
.ମଧ୍ୟ	generic	VeriSign Sarl
.ভারত	country-code	National Internet eXchange of India
.ভারত	country-code	National Internet Exchange of India
.八卦	generic	Zodiac Gemini Ltd
.موقع	generic	Suhub Electronic Establishment
.বাংলা	country-code	Posts and Telecommunications Division
.公益	generic	China Organizational Name Administration Center
.公司	generic	Computer Network Information Center of Chinese Academy of Sciences (China Internet Network Information Center)

O que significa “Aceitação Universal”?

UA (Universal Acceptance, Aceitação Universal) é o estado em que todos os nomes de domínio e endereços de e-mail válidos são aceitos, validados, armazenados, processados e exibidos de maneira correta.



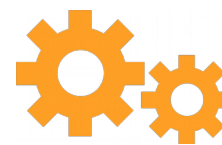
Aceitar



Validar



Armazenar



Processar



Mostrar

Referências

- O papel da ICANN na gestão dos identificadores únicos da Internet | Material:
[Funções IANA \[icann.org\]](#);
[Guia de Participação \[icann.org\]](#)
- Implementação da KSK no DNSSEC Material:
<https://www.icann.org/resources/pages/ksk-rollover-2016-07-27-pt> [icann.org]
- Aceitação Universal | Material:
[Artigo em Português \[itforum365.com.br\]](#);
[Guia rápido \[uasg.tech\]](#);
[Introdução a Aceitação Universal \[uasg.tech\]](#)
- Grupo dos Provedores na ICANN | Material:
<http://www.ispcp.info/>

Muito obrigado !



One World, One Internet

Visit us at icann.org



[@icann](https://twitter.com/icann)



facebook.com/icannorg



youtube.com/icannnews



flickr.com/icann



linkedin/company/icann



slideshare/icannpresentations



soundcloud/icann