Tópicos sobre DNS

Daniel Fink daniel.fink@icann.org

IX (PTT) Fórum Regional – Arcaju
Setembro2018

O que é a ICANN?

ICANN

Corporação da Internet para Designação de Nomes

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

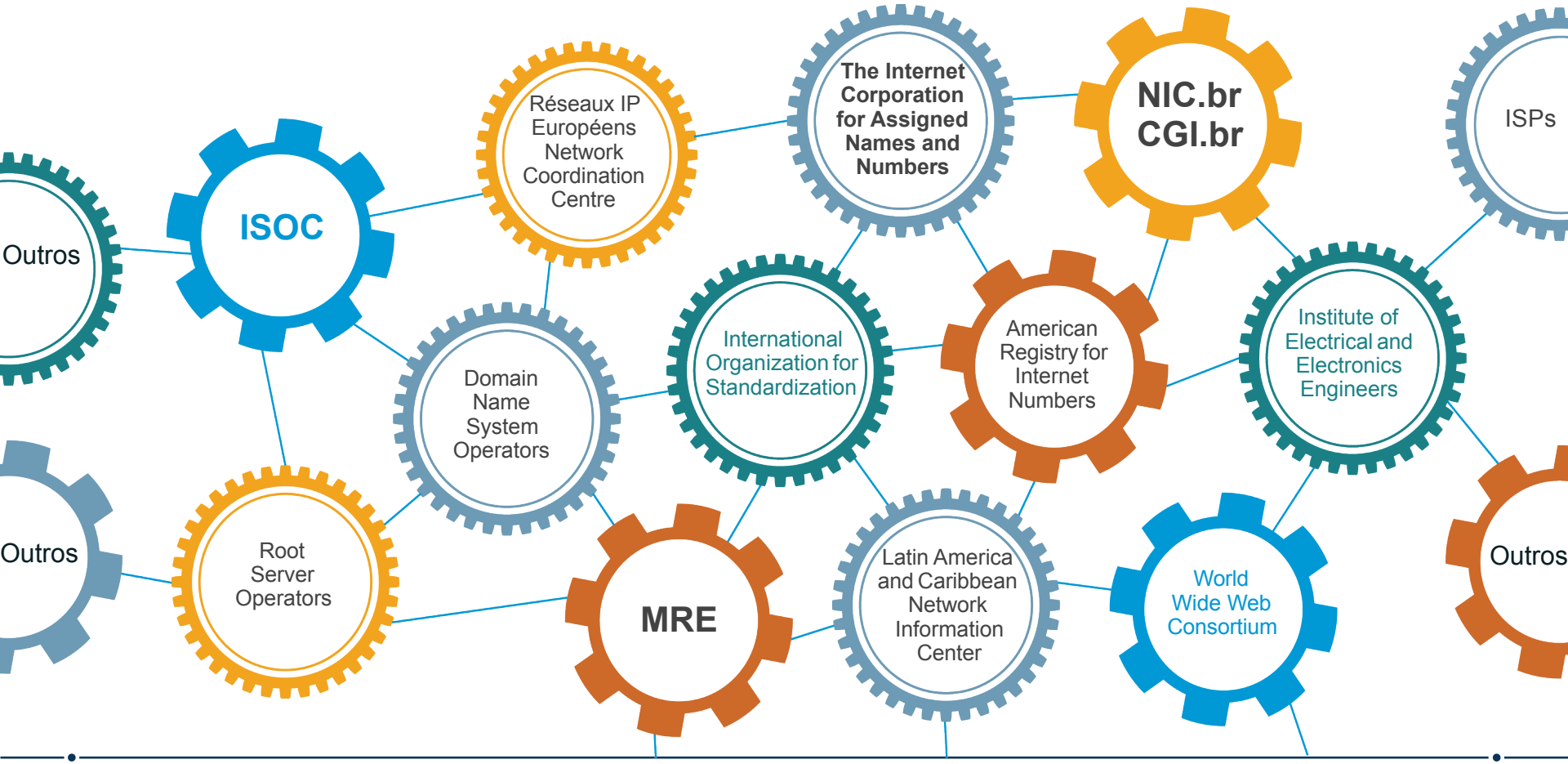
Ao desempenhar sua missão, a ICANN atuará de forma a cumprir e refletir seus compromissos e a respeitar seus valores essenciais

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

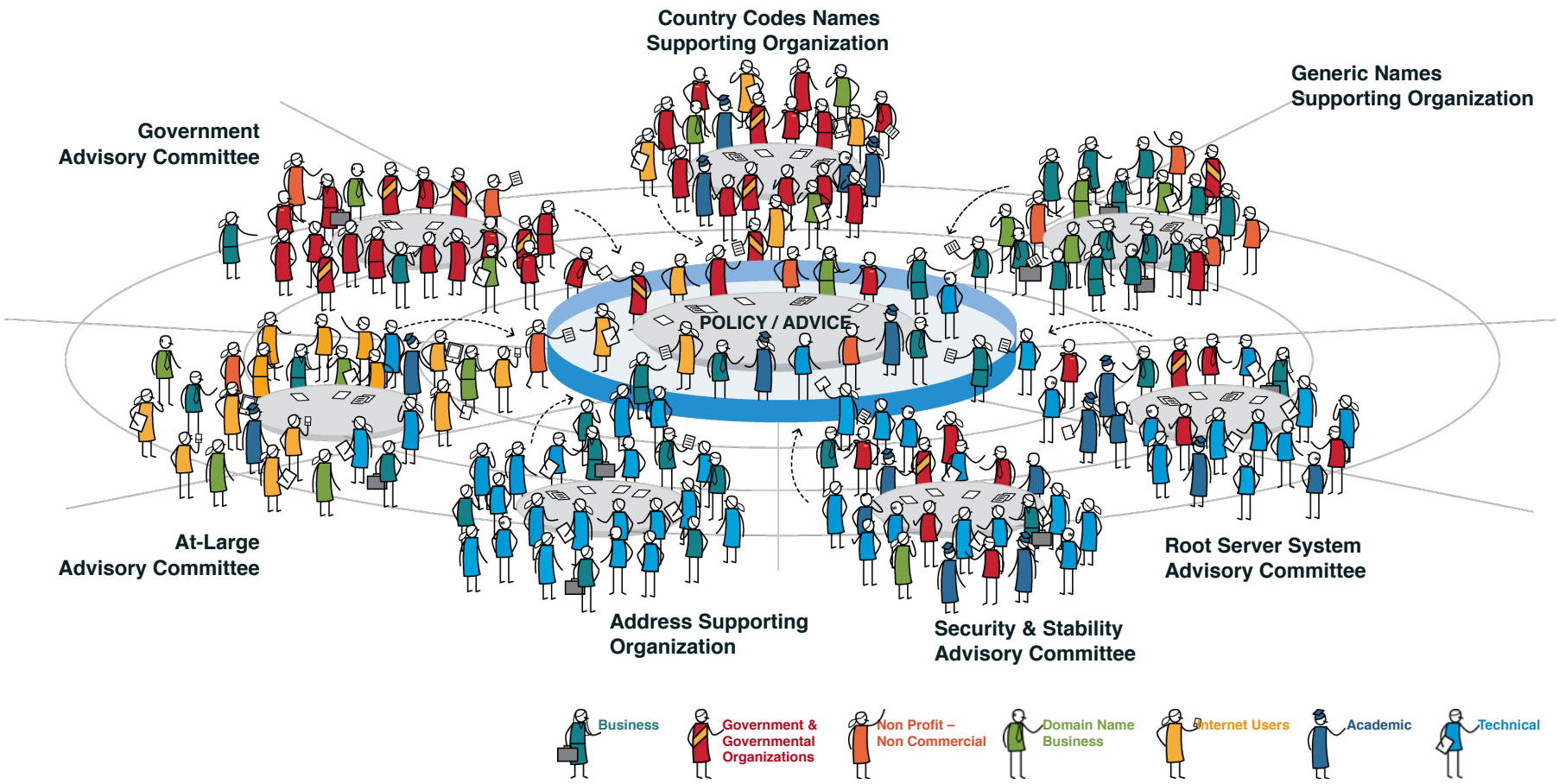
Nossos parceiros

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



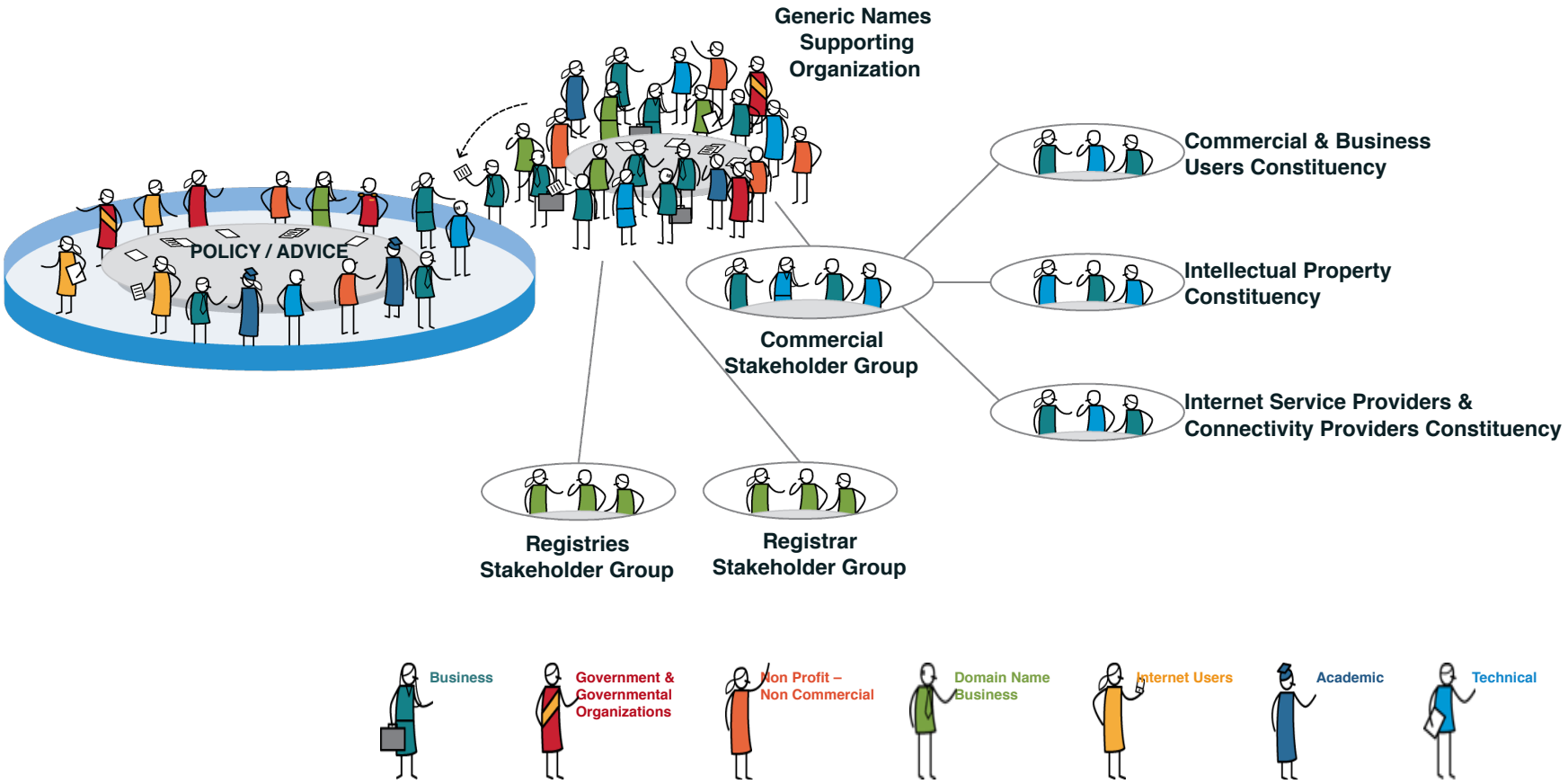
Estrutura da ICANN

Comunidade Multissetorial ICANN



Comunidade Multistakeholder ICANN

Setor Privado



O grupo dos provedores na ICANN

ICANN | ISPCP

Internet Service Providers & Connectivity Providers

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

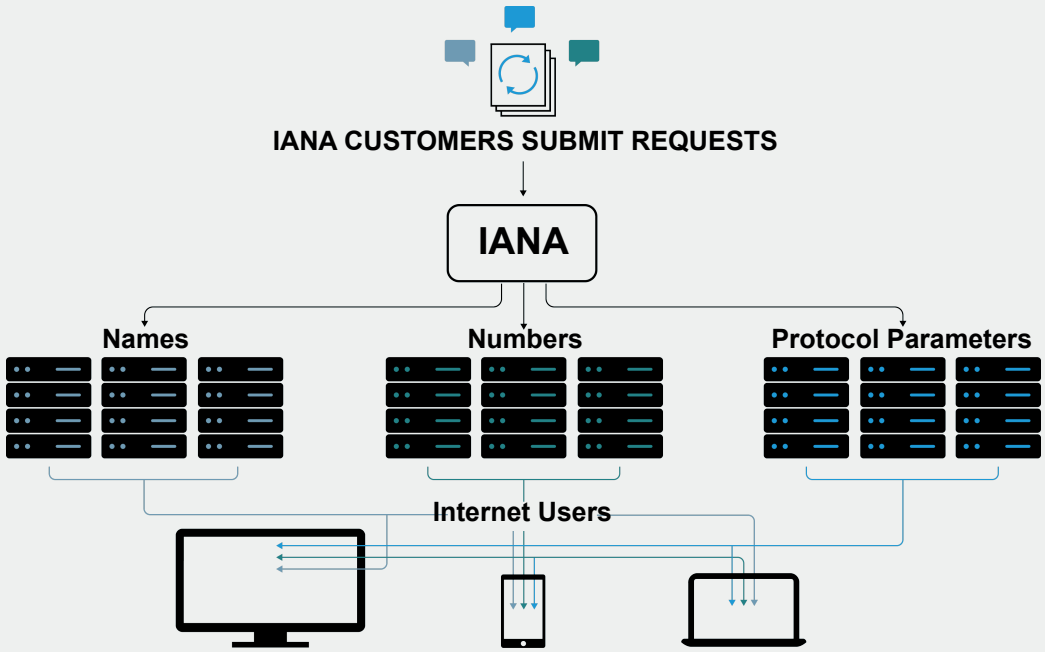
- Impacto do lançamento de novos nomes de domínio genéricos
- Universal Acceptance
- Impactos dos novos gTLD's

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 autonomos, servidores-raiz de números de domínio DNS e outros recursos relativos aos protocolos de Internet.



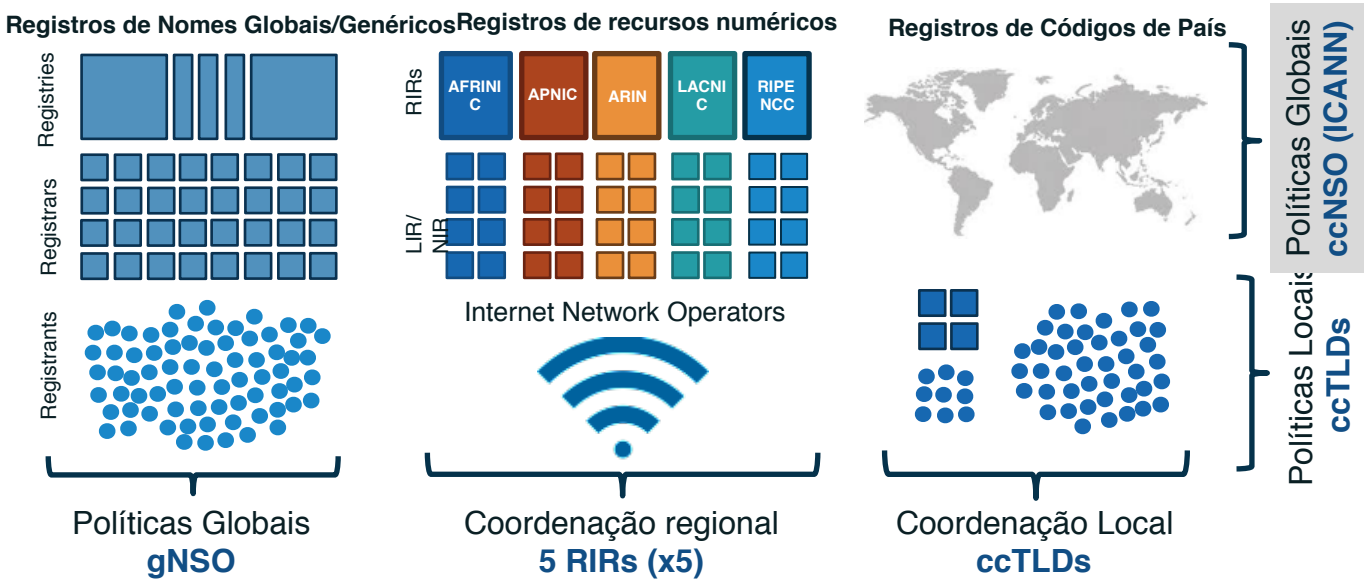
Essas funções incluem:

- 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.

Resumindo

Framework de Desenvolvimento de Políticas de Identificadores



- Altamente recomendável acompanhar e participar:

ICANN

lacnic

nic.br Núcleo de Informação e Coordenação do Ponto BR

cgi.br Comitê Gestor da Internet no Brasil

Aspectos técnicos

Estrutura do DNS

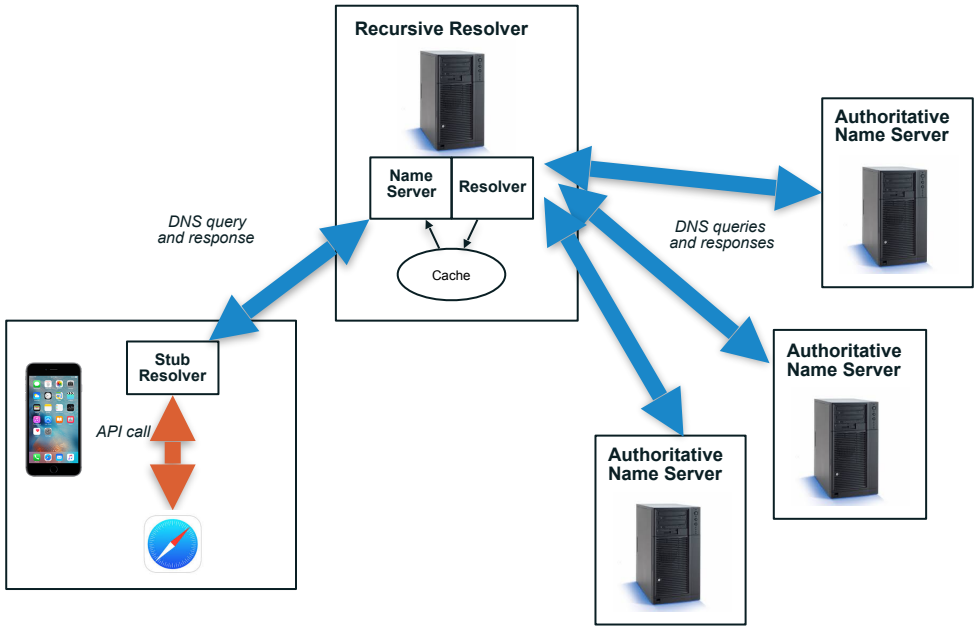
DNS em um slide

- 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



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)

The root-servers.org Web Site

root-servers.org

ARL DISA DoD NIC ISC NASA Ames UMD Cogent USC-ISI Verisign
WIDE ICANN RIPE NCC Netnod

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

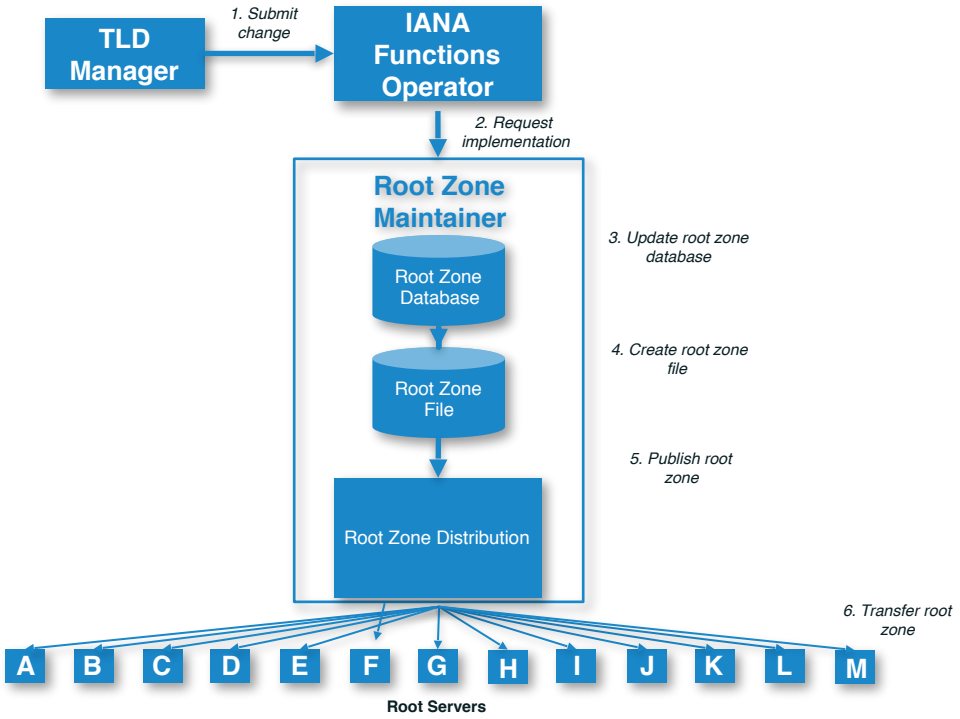
meeting agendas see all agenda items

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)

L-root instalados pelo NIC.br: **14**

nic.br
Núcleo de Informação e Coordenação do Ponto BR

Processo de mudanças na Zona Raiz



DNSSEC

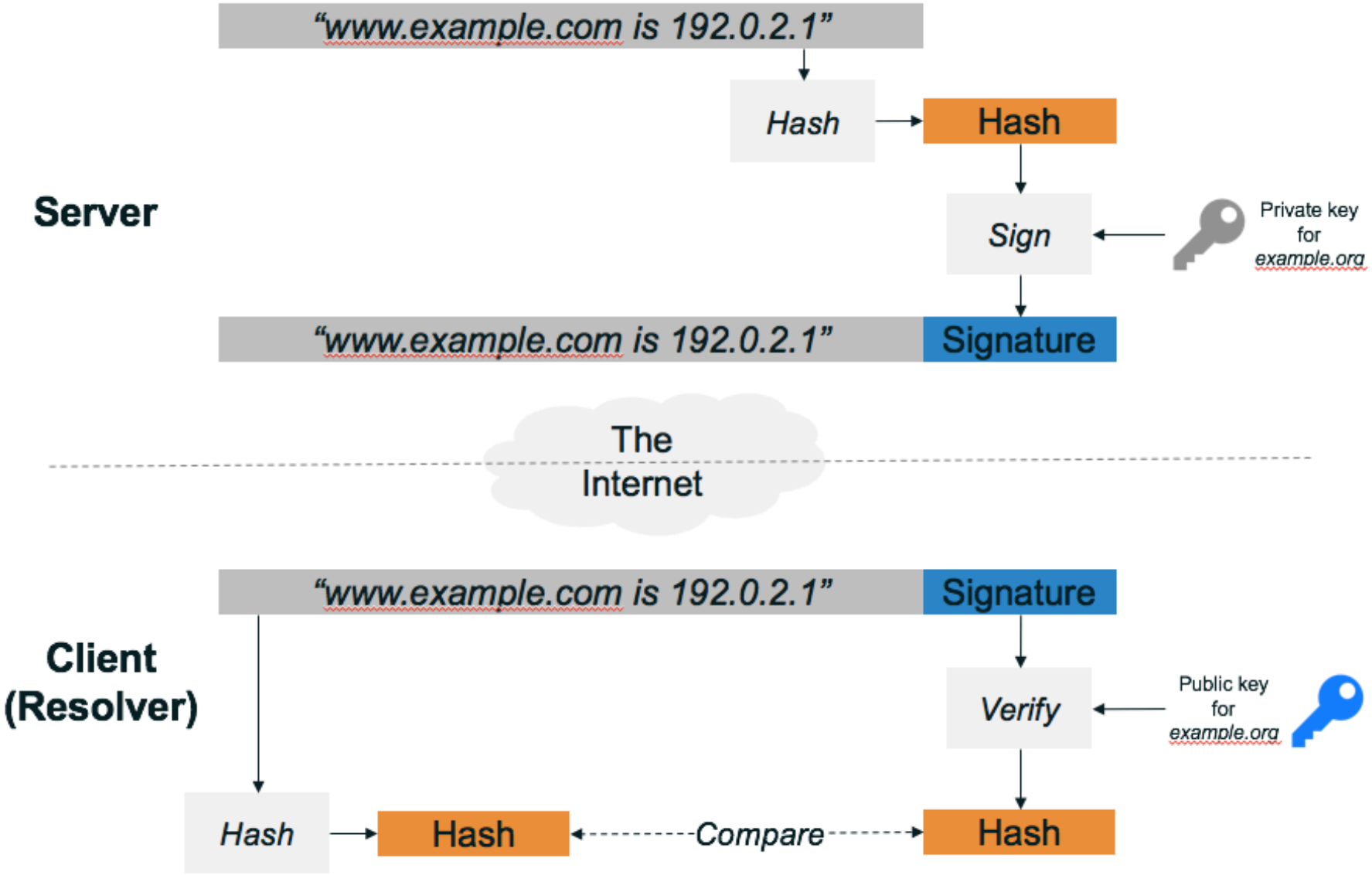
Implementação

da nova Chave de Assinatura de Chaves (KSK)

O que é DNSSEC?

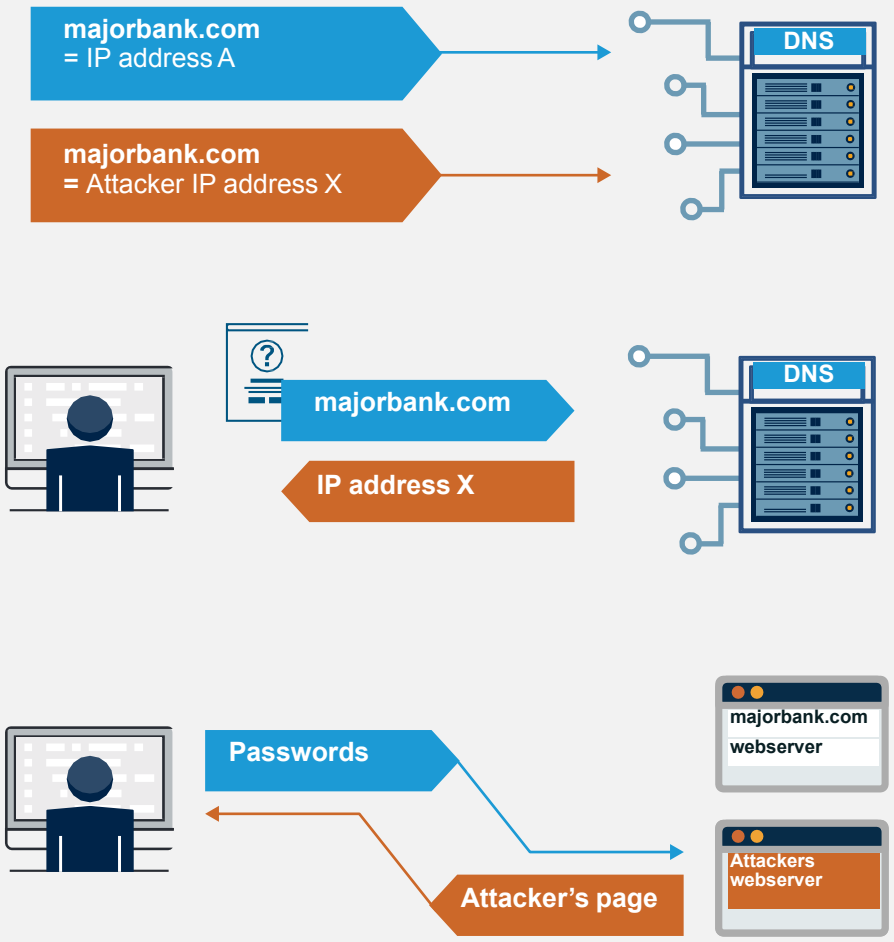
- DNSSEC = **“DNS Security Extensions”**
- É um protocolo que está sendo implantado atualmente para proteger o Sistema de Nomes de Domínio (DNS).
- O DNSSEC adiciona segurança ao DNS ao incorporar criptografia de chave pública na hierarquia do DNS, resultando em uma PKI (Public Key Infrastructure, infraestrutura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

Criptografia de Chave Pública e DNSSEC

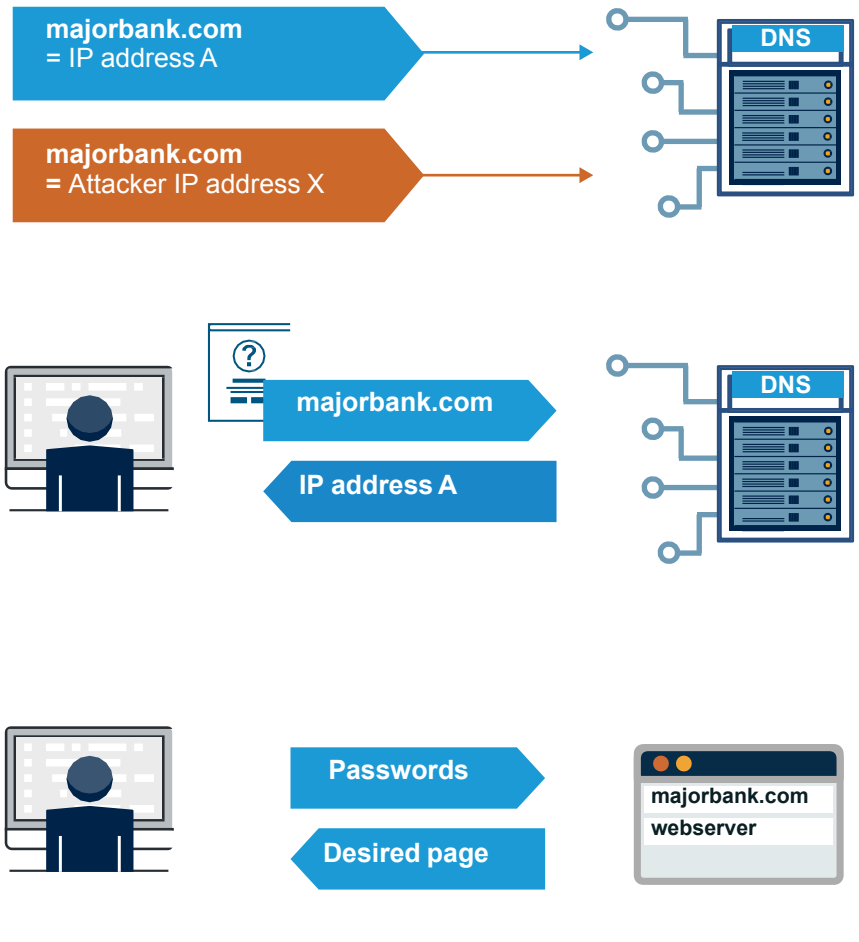


Como DNSSEC funciona?

Sem DNSSEC



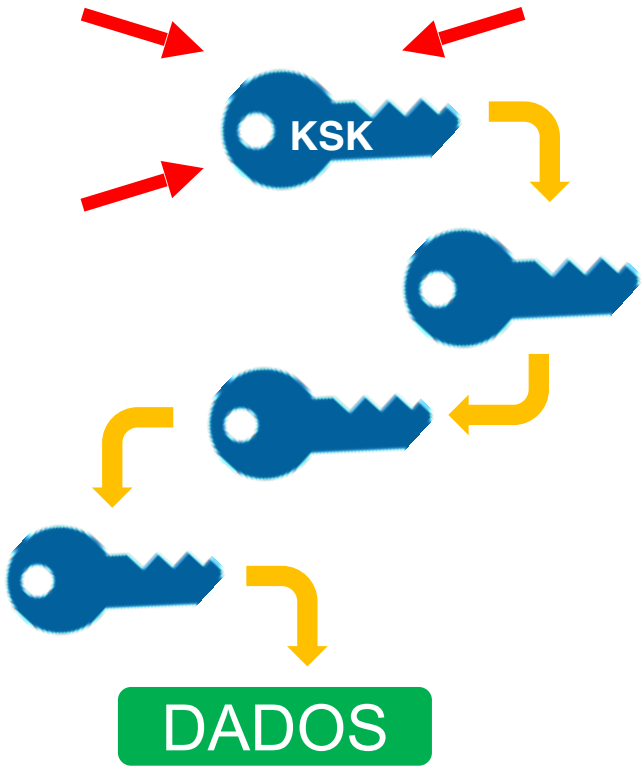
Com DNSSEC



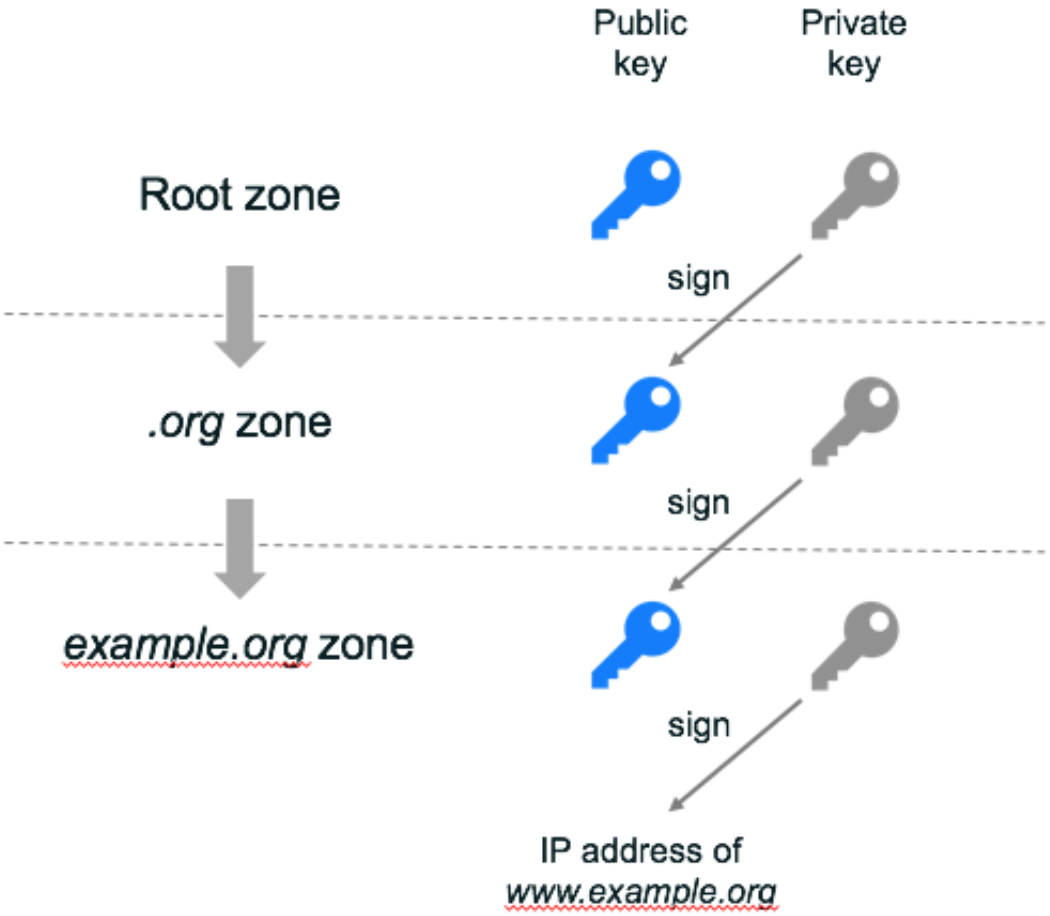
Implementação da KSK: Uma Visão Geral

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



A KSK é o ponto de partida de confiança



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)

Por que você precisa se preparar

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 resolvedores de validação de DNSSEC que poderão ser afetados pela implementação da KSK
- Se esses resolvedores 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

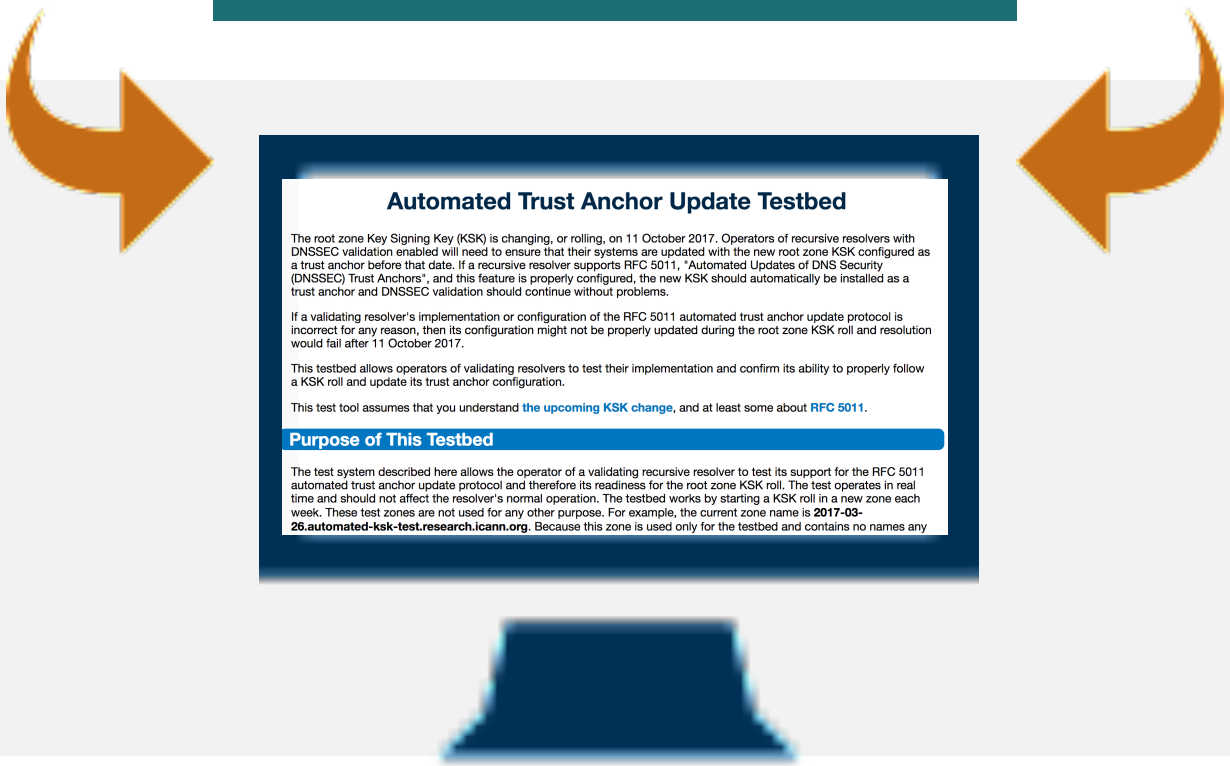
Se a validação de DNSSEC está ativada ou planejada no seu sistema

- 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



Reconhecimento da KSK-2017

- **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

A KSK-2017 em um registro de recurso de DNSKEY

◉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:

```
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0Ezr
AcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf
5/Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hOA2hzCTMj
JPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmR
LKBP1dfwhYB4N7knNnulqQxA+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=
```

Links e documentos importantes

- **Página principal: http://www.icann.org/kskroll**

- **Manual Geral sobre o que pode acontecer durante a substituição da KSK** https://www.icann.org/news/announcement-2018-08-27-pt

- **Instruções para atualizar as âncoras de confiança em softwares**

https://www.icann.org/dns-resolvers-updating-latest-trust-anchor

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 !

ICANN

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann