# O que esperar durante a implementação da KSK de raiz

Escritório de CTO da ICANN

22 de agosto de 2018

# Resumo executivo

Após o início da implementação da KSK (atualmente planejado para 11 de outubro de 2018), uma pequena porcentagem dos usuários da Internet deverá ter problemas para resolver alguns nomes de domínio. No momento, existe um número pequeno de DNSSEC (Domain Name System Security Extensions, Extensões de Segurança do Sistema de Nomes de Domínio) que validam resolvedores recursivos que estão configurados incorretamente, e alguns dos usuários que dependem desses resolvedores terão problemas. Este documento descreve quais usuários terão problemas e, entre eles, que tipos de erros eles verão em diversas situações.

- Os usuários que dependem de um resolvedor que não executa a validação de DNSSEC não observarão nenhuma alteração após a implementação.
- Os usuários que dependem de um resolvedor que tenha a nova KSK não observarão nenhuma alteração após a implementação.
- Se os resolvedores não tiverem a nova KSK na configuração da âncora de confiança, o usuário provavelmente começará a ver os efeitos disso em até 48 horas após a implementação.
- É impossível prever quando os operadores dos resolvedores afetados perceberão os erros de validação.

- Algumas análises de dados sugerem que mais de 99% dos usuários cujos resolvedores executam validação não serão afetados pela implementação da KSK.

# 1. Introdução

A Organização ICANN tem comunicado publicamente a futura implementação da KSK da zona raiz do DNS há alguns anos.[1] Durante o período para comentários públicos mais recente sobre os planos revisados para a implementação,[2] muitos membros da comunidade solicitaram mais detalhes sobre o processo. O Organização ICANN concordou em publicar mais materiais para ajudar na preparação para a implementação.[3] Este documento faz parte desse compromisso.

Houve uma certa confusão em diversas comunidades quando ao que será (e não será) visto após a implementação. Este documento apresenta detalhes sobre o que é esperado assim que a KSK for implementada.

[1] http://www.icann.org/kskroll
[2] https://www.icann.org/public-comments/ksk-rollover-restart-2018-02-01-en
[3] https://www.icann.org/en/system/files/files/report-comments-ksk-rollover-restart-23apr18-en.pdf

O documento é destinado a vários públicos-alvo. Os três principais são:

- Operadores de resolvedores com validação que querem saber o que esperar após a implementação;
- Membros da imprensa sem conhecimento técnico, entre outros, que pretendem escrever sobre a implementação antes e após a execução dela;
- Pesquisadores que pretendem monitorar o DNS em busca de indícios de falha nos resolvedores após a implementação.

É importante observar que este documento talvez não seja útil para os usuários que têm apenas um resolvedor que já está pronto para a implementação. Após a implementação, esses usuários não observarão nenhuma alteração na experiência deles com o DNS nem com a Internet em geral. Isso também ocorrerá para os usuários cujos resolvedores não executam a validação de DNSSEC. No momento, a estimativa é de que aproximadamente dois terços dos usuários utilizam resolvedores que ainda não executam a validação de DNSSEC.

A implementação deverá ser realizada em 11 de outubro de 2018. A data da implementação da KSK será confirmada pela Diretoria da ICANN antes. A implementação estava originalmente planejada para 11 de outubro de *2017*, mas foi adiada devido ao recebimento de dados imprecisos um pouco antes dessa data.[4]

As Seções 2 e 3 deste documento descrevem o que acontecerá após a implementação aos resolvedores com validação que estão preparados para esse processo e aos que não estão. A Seção 4 descreve o que poderá ser observado pelos pesquisadores que estão monitorando o tráfego do sistema de servidores-raiz do DNS. Neste documento são usadas frases não definitivas para descrever o que ocorrerá após a implementação. Elas são usadas porque não há como ninguém, além do próprio operador de um determinado resolvedor, prever precisamente o software executado pelo resolvedor. Além disso, é impossível sequer saber se um resolvedor está configurado corretamente para a implementação.

***Observação importante para operadores de resolvedores***: Todos os operadores de resolvedores com validação que lerem este documento deverão confirmar imediatamente se estão preparados para a implementação verificando as âncoras de confiança usadas.[5] Se não estiverem prontos, os operadores deverão atualizar as âncoras de confiança com a versão mais recente delas o quando antes.[6] Os operadores de resolvedores que não executam a validação de DNSSEC já estão prontos para a implementação.

## 1.1 Definição de implementação da KSK de raiz

A zona raiz do DNS foi assinada com DNSSEC em 2010. A zona raiz do DNS tem dois tipos de chaves: as ZSKs (Zone-Signing Keys, Chaves de Assinatura de Zona), que assinam os dados principais na zona raiz; e as KSKs (Key Signing Keys, Chaves de Assinatura de Chave), que assinam apenas o conjunto de chaves da raiz (ZSKs e KSKs) na zona raiz. Uma nova ZSK é publicada a cada três meses. Cada nova ZSK é assinada por uma KSK mais antiga.

[4] https://www.icann.org/news/announcement-2017-09-27-en
[5] https://www.icann.org/dns-resolvers-checking-current-trust-anchors
[6] https://www.icann.org/dns-resolvers-updating-latest-trust-anchor

A implementação ocorre quando a KSK da raiz é alterada e essa nova KSK começa a assinar o conjunto de chaves da raiz para a zona. No momento da implementação, a KSK original será aposentada e a nova KSK começará a ser usada. A primeira KSK é chamada de KSK-2010 (ainda em uso). A nova KSK é chamada de KSK-2017. Após a implementação, a KSK-2010 não assinará mais o conjunto de chaves da raiz, e a KSK-2017 começará a assinar o conjunto de chaves da raiz.

## 1.2 Âncoras de confiança

Para entender como ocorrerá a implementação, é importante também entender como os resolvedores com validação confiam na KSK da raiz. Cada resolvedor com validação é configurado com um conjunto de *âncoras de confiança*, que são cópias das chaves ou identificadores de chave que correspondem à KSK da raiz. As âncoras de confiança geralmente são configuradas automaticamente pelos fornecedores de software, pelos resolvedores configurados para atualizar automaticamente as âncoras de confiança usando o processo descrito na RFC 5011[7] ou ainda pelos operadores de resolvedores que acrescentam manualmente uma nova KSK ao repositório de âncoras de confiança do resolvedores.

Antes da KSK-2017, todos os resolvedores com validação tinham apenas a KSK-2010 configurada como âncora de confiança. Após a criação e a publicação da KSK-2017, a maioria dos operadores de resolvedores adicionaram a KSK-2017 manualmente à configuração da âncora de confiança do resolvedor ou essa alteração foi feita pelo software usado por eles (como, por exemplo, pelo processo de atualização automática da RFC 5011) ou pelo fornecedor do software. No entanto, alguns operadores de resolvedores não atualizaram a configuração e agora não estão prontos para a implementação porque ainda têm apenas a KSK-2010 como âncora de confiança. Após a implementação, esses operadores de resolvedores não terão âncoras de confiança válidas.

# 2. Resolvedores preparados para a implementação

Os resolvedores que estão preparados para a implementação já têm a KSK-2017 configurada como âncora de confiança. Quando a implementação for executada, esses resolvedores continuarão funcionando da mesma forma que antes da implementação, porque a nova KSK da raiz já é confiada para assinar o conjunto de chaves da raiz. É possível que alguns softwares de resolvedores observem nos registros operacionais que a implementação foi realizada, mas essas entradas de registro (se houver) provavelmente não serão vistas, a menos que o operador esteja procurando especificamente por elas.

Os usuários de resolvedores que estão preparados para a implementação não perceberão nenhuma diferença após a implementação. As respostas recebidas para consultas normais serão idênticas antes e após a implementação. De acordo com uma pesquisa recente da APNIC,[8] mais de 99% dos usuários cujos resolvedores executam a validação de DNSSEC utilizam resolvedores que estão preparados para a implementação.

[7] https://datatracker.ietf.org/doc/rfc5011/
[8] http://www.potaroo.net/ispcol/2018-04/ksk.html

A maioria dos usuários da Internet tem mais de um resolvedor do DNS configurado. Se qualquer um dos resolvedores configurados pelo usuário estiver preparado para a implementação, o software do usuário encontrará esse resolvedor após a implementação e continuará utilizando-o. É possível que isso deixe a resolução do DNS um pouco lenta, já que o sistema continuará tentando o resolvedor que não está preparado antes de trocar para o resolvedor que está preparado, mas o usuário ainda assim receberá a resolução do DNS.

# 3. Resolvedores não preparados para a implementação

Se um resolvedor tiver apenas a KSK-2010 configurada como âncora de confiança, após a implementação, esse resolvedor começará a apresentar erros na validação de respostas recebidas dos servidores autoritativos. No entanto, é impossível prever quando essa falha começará a ocorrer.

Embora a publicação no DNS seja instantânea, é possível que um determinado resolvedor demore um pouco para ver um novo registro publicado. Cada registro no DNS tem um “tempo de vida” (geralmente chamado de *TTL*), durante o qual o resolvedor não tentará acessar uma versão mais recente do registro. Após a implementação, os resolvedores provavelmente ainda terão uma versão em cache da assinatura feita pela KSK-2010 e, sendo assim, continuarão validando com sucesso, pelo menos durante um período.

## 3.1 As falhas ocorrerão quando não for possível validar a ZSK

Sempre que um resolvedor com validação recebe uma resposta de um servidor de nome autoritativo, ele verifica a assinatura na resposta. O resolvedor salva o status da validação da assinatura em cada nome no cache. Para validar a assinatura em um nome como “www.example.com”, o resolvedor precisa validar a assinatura na raiz, em “.com”, no caso de “example.com” e “www.example.com”. Os resolvedores geralmente colocam essas validações em cache para que elas não sejam executadas em cada nome. A maioria dos resolvedores executa as validações apenas quando o status da validação talvez tenha sido alterado.

O TTL dos registros de KSK e ZSK é de 48 horas. Se um resolvedor receber o conjunto de chaves da raiz e o validar *um pouco antes* da implementação, esse resolvedor não perceberá que ela ocorreu por aproximadamente dois dias, porque ele não buscará uma nova KSK até receber a primeira consulta após a expiração do TTL do conjunto de chaves da raiz. Em um resolvedor normal com apenas alguns usuários, essa consulta ocorrerá após alguns minutos (ou até mesmo segundos) depois que o TTL dos registros de DNSKEY expirar. Em um resolvedor com apenas um usuário, é possível que a primeira consulta leve algumas horas, ou até mesmo dias, após a expiração do TTL do conjunto de chaves da raiz.

É importante observar que essa é uma descrição simplificada do que realmente ocorre. Por exemplo, alguns resolvedores têm um limite máximo de TTL, o que pode fazer com que esses resolvedores percebam a implementação da chave antes. Outras opções de configuração também podem afetar o momento em que o resolvedor verá a implementação.

## 3.2 Quais usuários verão quando todos os resolvedores apresentarem falhas

Em algum momento durante as primeiras 48 horas após a implementação, algumas consultas do DNS dos usuários começarão a apresentar falhas porque elas farão com que o resolvedor busque o conjunto de chaves da raiz novamente. Conforme explicado acima, não é possível prever quando os primeiros resultados apresentarão falhas durante esse período de 48 horas.

Quando elas ocorrerem, se o usuário tiver vários resolvedores configurados (como é o caso da maioria), o software de sistema tentará acessar os outros resolvedores configurados. É possível que isso deixe a resolução do DNS um pouco lenta, já que o sistema continuará tentando o resolvedor que não está preparado antes de trocar para o resolvedor que está preparado, mas o usuário ainda assim receberá a resolução do DNS e talvez nem perceba essa lentidão. No entanto, se todos os resolvedores do usuário não estiverem preparados para a implementação (como, por exemplo, se todos eles forem gerenciados por uma única organização e ela não tiver preparado nenhum dos resolvedores), o usuário começará a observar falhas em algum momento durante as primeiras 48 horas após a implementação.

Os usuários verão sintomas diferentes de erros dependendo do programa executado e de como ele reage às pesquisas de DNS com falha. Nos navegadores, é possível que uma página da Web fique indisponível (ou talvez apenas as imagens em uma página da Web que já estiver sendo exibida apresentem falha). Nos programas de e-mail, é possível que os usuários não recebam novas mensagens ou algumas partes do texto apresentem erros. O número de falhas aumentará até que nenhum programa consiga mostrar novas informações da Internet.

Observe que o termo “usuários” aqui não se refere apenas a seres humanos. Os sistemas automatizados que também estiverem usando resolvedores não preparados para a resolução do DNS começarão a apresentar falhas, com um efeito possivelmente catastrófico.

Depois que o operador do resolvedor corrigir os erros na validação (seja adicionando a KSK-2017 como âncora de confiança ou desativando a validação), a experiência dos usuários na Internet voltará ao normal quase que imediatamente.

## 3.3 Como os operadores de resolvedores ficarão sabendo sobre a falha

Os operadores de resolvedores que tiverem configurado um software de monitoramento do sistema para encontrar erros sérios serão alertados imediatamente após o resolvedor buscar uma nova cópia do conjunto de chaves da raiz e não conseguir executar a validação. Esse tipo de monitoramento é a melhor forma de um operador detectar rapidamente a falha e iniciar o processo de recuperação.

Se o operador não monitorar ativamente a presença de erros sérios, é provável que ele não detecte a falha na validação até que os sistemas automatizados que dependem do resolver comecem a falhar ou que os usuários comecem a reclamar de interrupções no serviço. Se, além disso, o operador usar apenas resolvedores com as configurações incorretas de âncoras de confiança, é possível que eles não recebam mensagens de e-mail enviadas a ele e talvez só fiquem sabendo do problema se receberem reclamações por telefone.

### 3.4 Recuperação após os efeitos de não estar preparado

Assim que os operadores descobrirem que a validação de DNSSEC está apresentando falhas, eles devem alterar a configuração do resolvedor para desativar temporariamente a validação de DNSSEC. Isso resolverá o problema imediatamente.

Depois, o operador deverá instalar, assim que possível, a KSK-2017 como âncora de confiança e ativar a validação de DNSSEC novamente. A Organização ICANN disponibiliza instruções para atualizar as âncoras de confiança em softwares comuns de resolvedores.[9]

# 4. O que os operadores de servidores-raiz verão

Após a implementação, os operadores de servidores-raiz começarão a ver um aumento significativo das consultas de resolvedores que não estão preparados para a implementação. Essas consultas provavelmente serão relacionadas ao DNSKEY da raiz (./IN/DNSKEY) e é possível que também incluam consultas para o registro de DS da zona .net (.net/IN/DS). Além disso, já que as respostas não podem ser validadas corretamente, elas não serão armazenadas em cache, o que resultará no aumento do tráfego em geral para os resolvedores que executam validação. Da mesma forma, os operadores de resolvedores que permitem o encaminhamento de outros resolvedores por eles provavelmente começarão a ver um aumento do número desse tipo de solicitação após a implementação.

Alguns pesquisadores já estão monitorando o tráfego do servidor raiz em busca de solicitações de DNSKEY da raiz para terem uma base de comparação do número normal de consultas por minuto. Essas estatísticas são encaminhadas à ICANN quase que em tempo real (uma vez por minuto) por 11 das 12 organizações de servidores-raiz. A ICANN continuará monitorando essas estatísticas após o início da implementação e enviará os resultados para os operadores de servidores-raiz e os demais membros da comunidade técnica do DNS.

# Anexo A: onde encontrar mais informações sobre a implementação

A principal fonte de informações sobre a implementação é:

http://www.icann.org/kskroll

Essa página tem um Guia Rápido sobre a Implementação da KSK, que é um conjunto abrangente de recursos sobre o DNSSEC, explica por que a comunidade optou pela implementação e inclui os planos para a implementação. Ela está disponível em inglês, espanhol, francês, russo, árabe, chinês, português, coreano e japonês.

Inscreva-se nesta lista de e-mails para participar da discussão sobre a implementação:

https://mm.icann.org/listinfo/ksk-rollover

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

# Anexo B: glossário

DNSSEC – Extensões do DNS que permitem a um servidor autoritativo assinar criptograficamente registros do DNS para que um resolvedor tenha certeza de que os dados no registro não foram alterados.[10]

KSK – Key Signing Key (Chave de Assinatura de Chave), refere-se à chave usada para assinar todas as chaves em uma zona.

Implementação – alteração de uma Chave de Assinatura de Chave em uma zona a partir de uma chave existente para uma nova.

TTL – refere-se ao “Time To Live” (Tempo de Vida) de um conjunto de registros no DNS. Quando um resolvedor recebe um conjunto de registros de um servidor autoritativo, ele geralmente armazena esses registros em cache pelo número de segundos indicado no TTL.

Validação – validação das assinaturas nos registros em uma zona protegida pelo DNSSEC. Os resolvedores executam uma validação para ter certeza de que os registros recebidos de um servidor autoritativo estão corretos.

ZSK – Zone Signing Key (Chave de Assinatura de Zona), refere-se à chave usada para assinar todos os registros em uma zona além das chaves (que são assinadas pela Chave de Assinatura de Chave).

[10] https://meetings.icann.org/en/marrakech55/schedule/sun-dnssec-everybody