Guia de Implementação do DNSSEC para ccTLD

Gabinete do Diretor de Tecnologia da ICANN

Yazid Akanho e Paul Muchene
OCTO-029
12 Novembro 2021

ÍNDICE

Este documento faz parte da série de documentos do Gabinete do Diretor Técnico Principal (OCTO) da ICANN. Consulte a página de publicações da OCTO para obter uma lista dos documentos da série. Se tiver alguma dúvida ou sugestão, sobre qualquer um destes documentos, envie-as para octo@icann.org.

Este documento apoia o objetivo estratégico da ICANN de melhorar a responsabilidade partilhada pela manutenção da segurança e estabilidade do Sistema de Nomes de Domínio (DNS), reforçando a coordenação do DNS em parceria com os intervenientes relevantes. Faz parte do objetivo estratégico da ICANN reforçar a segurança do DNS e do sistema de servidores raiz do DNS (RSS).

NOTA DA VERSÃO PORTUGUESA

Este documento é uma tradução para português do documento original publicado pela ICANN. A tradução apresentada foi realizada no âmbito do programa de capacitação digital da LusNIC e CDA/ICANN, sendo esta fornecida apenas para fins informativos. Em caso de divergência, inconsistência ou dúvida de interpretação, a versão original prevalece.

A LusNIC agradece à ICANN, entidade responsável pelo documento original, pela produção e disponibilização destes conteúdos, que serviram de base à presente tradução para português, realizada com o objetivo de apoiar a capacitação e a partilha de conhecimento entre os membros da comunidade LusNIC.

1 Introdução

Nos últimos anos, a segurança tem-se tornado uma questão cada vez mais importante na Internet. Especificamente para o Sistema de Nomes de Domínio (DNS), foram propostos e desenvolvidos vários protocolos de segurança ao longo dos anos, sendo o Domain Name System Security Extensions (DNSSEC) um dos protocolos mais importantes. O DNSSEC ajuda a proteger as respostas do DNS, acrescentando a autenticação da origem dos dados e a proteção da integridade dos dados.

A zona raiz do DNS gerida pela ICANN foi assinada pela primeira vez com o DNSSEC em julho de 2010. À data de publicação deste guia, todos os Top-Level Domains genéricos (gTLD) serão assinados com DNSSEC, em parte devido a obrigações contratuais com a ICANN; por outro lado, apenas cerca de 60 % dos Top-Level Domains com código de país (ccTLD's) foram assinados. Uma das razões que pode explicar esta tendência a nível dos ccTLD's é a falta de visibilidade dos gestores de ccTLD's no processo de proteção das suas zonas com DNSSEC.

Neste sentido, o Gabinete do Diretor de Tecnologia (OCTO) da ICANN publicou este guia para ajudar os operadores de registry ccTLD a melhor inteirarem-se sobre processo que os pode ajudar a assinar as suas zonas com DNSSEC. Não abrange o segundo aspeto do DNSSEC, que é a validação que ocorre principalmente nos resolvedores recursivos do DNS, normalmente localizados em Fornecedores de Serviços de Internet (ISP), em grandes operadores de nuvens públicas ou em redes empresariais.

1.1 Público-alvo deste documento

Este guia destina-se principalmente a fornecer aos gestores de registry ccTLD, colaboradores, partes interessadas, em particular registrars, registrants e qualquer outra pessoa, uma visão geral do DNSSEC e da forma como este pode ser implementado por um registry na assinatura de zonas. Este documento não apresenta detalhes técnicos de configuração, servindo como um guia para um entendimento básico do protocolo DNSSEC, dos pré-requisitos e das considerações de implementação na assinatura de zonas de um ccTLD.

Mesmo que já esteja a operar um TLD assinado com DNSSEC, este documento poderá ajudar a identificar pontos de melhoria, como as melhores práticas algorítmicas atuais ou a documentação adequada do serviço DNS geral. Se é um operador de ccTLD ou administra zonas sob um ccTLD assinado, este guia pode ajudar a dar os primeiros passos. Apesar de todos os operadores de gTLD já terem assinado as suas zonas, também podem obter informações sobre as melhores práticas operacionais do DNSSEC descritas neste documento e utilizá-lo como base para sensibilizar os seus registrars e registrants para o DNSSEC.

Há vários documentos sobre os aspetos teóricos, técnicos e operacionais do DNSSEC, e este guia cita vários como referência. Os leitores são, por conseguinte, convidados a consultar os documentos citados se pretenderem aprofundar os seus conhecimentos ou compreensão de um ou outro aspeto relacionado com o DNSSEC.

2 DNSSEC e o seu valor para o DNS

O Sistema de Nomes de Domínio (DNS) é um sistema de nomes hierárquico, distribuído e descentralizado para a Internet. À semelhança de uma lista telefónica que traduz nomes para números de telefone, o DNS ajuda a converter informações de nomes de domínio em endereços IP e vice-versa. O DNS é considerado um serviço crítico na Internet, se bem que não foi originalmente concebido com

fortes mecanismos de segurança para garantir a integridade e a autenticidade dos seus dados. Ao longo dos anos, foram descobertas várias vulnerabilidades que ameaçam a fiabilidade e a credibilidade do DNS, e o DNSSEC ajuda a resolver algumas delas.

O DNSSEC é definido e especificado principalmente em três documentos de normas da Internet: RFC 4033, *DNS Security Introduction and Requirements*; RFC 4034, *Resource Records for the DNS Security Extensions;* e RFC 4035, *Protocol Modifications for the DNS Security Extensions*. O DNSSEC utiliza criptografia de chave pública (a geração de pares de chaves públicas e privadas) para adicionar ao DNS capacidades de autenticação da origem dos dados, integridade dos dados, verificação e negação de existência autenticada. Especificamente, acrescenta assinaturas digitais e um novo conjunto de tipos de registos de recursos e bits de cabeçalho de mensagem (bandeiras) ao DNS, que podem ser utilizados para verificar as respostas do DNS de uma zona assinada. É de salientar que o DNSSEC não encripta quaisquer dados de mensagens DNS, logo não fornece confidencialidade.

Quando um domínio é assinado com DNSSEC, as assinaturas digitais são geradas pelo administrador de zona utilizando uma chave privada e publicadas como um registo de Assinatura de Registo de Recursos (RRSIG) no ficheiro de zona como parte dos dados de zona do domínio. Quando um resolvedor recursivo sensível à segurança, também conhecido como resolvedor de validação, envia uma consulta DNS para um servidor autoritativo do domínio assinado, a resposta DNS contém o registo de recursos em texto não encriptado ou num formato não encriptado e a respetiva assinatura digital associada. O resolvedor utiliza depois a assinatura digital que recebeu para validar esta resposta DNS. Para este efeito, o resolvedor de validação também solicita outras informações relacionadas com o DNSSEC, como a chave pública armazenada no registo DNSKEY e publicada pelo administrador do domínio nos dados da zona.

3 Pré-requisitos e requisitos para a implementação do DNSSEC

3.1 Documentação do sistema existente

Devido ao papel crítico que o DNS desempenha na Internet e à necessidade de evitar a interrupção do serviço em todas as circunstâncias, é importante manter uma documentação atualizada que descreva a infraestrutura, as operações e os processos do DNS. O DNSSEC, por outro lado, acrescenta um certo nível adicional de complexidade à infraestrutura e operações do DNS existentes. Assim, manter a documentação atualizada é crucial para garantir que está disponível para referência uma imagem clara do sistema existente. Isto também permite a continuidade operacional em caso de rotação de colaboradores ou de atualização da infraestrutura.

Recomendamos que a documentação resuma dois aspetos principais: as políticas de

governação do ccTLD, e os aspetos operacionais e técnicos do serviço.

Para além disso, é aconselhável que o documento contenha o máximo de informações possível, omitindo quaisquer dados sensíveis ou confidenciais, como nomes de utilizador e palavras-passe, que possam ser utilizados para efetuar ataques contra o registry.

Os aspetos de governação do documento podem abranger tópicos como:

- a visão geral e a estrutura do ccTLD;
- modelo(s) de registo: 3R (registry, registrar e registrant), 2R (apenas registry e registrant) ou outros modelos;
- contactos técnicos e administrativos do registry;
- recursos humanos, funções, responsabilidades e contactos das pessoas envolvidas no processo de tomada de decisões técnicas do registry;
- uma lista de registrars e respetivas informações de contacto.

Os aspetos técnicos e operacionais do documento podem abranger temas como:

- número de servidores de nomes autoritativos (NSes) primários e secundários com os respetivos endereços IP, informações de contacto do TLD (endereços de telefone e de correio eletrónico), protocolos utilizados entre o registry e os registrars, como o Extensible Provisioning Protocol (EPP), o software e o hardware que implementam as funções do registry, incluindo a base de dados do registry, o Registration Data Access Protocol (RDAP) e/ou os servidores Whois, entre outras informações técnicas;
- acesso dos utilizadores e inventário de privilégios apenas estritamente disponíveis para um número limitado de pessoas autorizadas;
- cópias de segurança e procedimentos de restauro;
- segurança: acesso físico, gestão de registos, controlos de acesso, gestão de palavras-passe, firewalls, integridade de ficheiros de zona e segurança de transferência de zona, entre outros;
- sistemas de monitorização: hardware, software, sincronização de zonas (entre NSes);
- estratégia de manutenção;
- Plano de Continuidade de Negócios e de Recuperação de Desastres.

3.2 Auditar a infraestrutura existente

Como referido anteriormente, a implementação do DNSSEC acrescenta um nível de complexidade à infraestrutura e às operações de DNS existentes. Por conseguinte, uma prática boa e segura seria efetuar uma auditoria à atual infraestrutura, operações e processos do sistema, através de uma entidade externa ou interna com competências e autonomia necessárias para identificar e partilhar as suas conclusões e eventuais lacunas. É essencial corrigir quaisquer deficiências no sistema atual antes ou em paralelo com a assinatura da zona. Assim, reduz-se o risco de as coisas se tornarem incontroláveis após a implementação do DNSSEC.

3.3 Redação de uma Política DNSSEC e Declarações de Práticas DNSSEC

3.3.1 O que é uma Política DNSSEC e uma Declaração de Práticas DNSSEC?

Há várias considerações e parâmetros a definir quando se assina um domínio, por exemplo, algoritmos de assinatura DNSSEC, tamanhos de chave, período de validade da assinatura e

frequência das atualizações de assinatura. No caso de uma zona com muitas delegações, uma boa prática consiste em documentar na íntegra e manter atualizados os conjuntos de parâmetros aplicáveis à zona e disponibilizá-los publicamente. Por conseguinte, devem ser tidos em consideração dois conceitos:

- **Política DNSSEC** (DP): estabelece os requisitos e normas de segurança a implementar numa zona assinada com DNSSEC. A DP constitui uma base para uma auditoria, acreditação ou avaliação de uma entidade, por exemplo, um registry. Cada entidade pode ser avaliada em relação a um ou mais DP que alega implementar. Em suma, a DP indica o que deve ser feito.
- **Declaração de Práticas DNSSEC** (DPS): trata-se de um documento de divulgação de práticas operacionais que pode apoiar e suplementar a Política DNSSEC (caso exista). Indica, a um nível elevado, a forma como um operador de zona e os seus parceiros de gestão de zona, caso existam, implementam procedimentos e controlos para cumprir os requisitos da DP aplicável. Ao contrário de uma DP, a DPS indica o que está efetivamente a ser feito.

Uma DP apresenta princípios gerais, ao passo que uma DPS fornece uma descrição dos procedimentos e controlos, o que a torna mais pormenorizada do que uma DP. Por outro lado, a política é normalmente redigida por uma autoridade política (gestor do TLD ou autoridade reguladora) e pode ser aplicável a uma ou mais zonas na hierarquia do DNS, enquanto que uma declaração de prática específica para uma única zona é redigida pelo operador da zona, descrevendo a forma como cumpre os requisitos de uma determinada política ou de um conjunto de políticas.

A título de exemplo, no contexto em que tanto o contacto administrativo como o contacto técnico de um ccTLD são entidades diferentes, o contacto administrativo pode publicar uma política que defina as normas e os requisitos a seguir, exigindo também que o contacto técnico publique uma declaração de práticas que descreva o modo como essas normas e requisitos serão cumpridos.

Em alternativa, um operador ou gestor de zona que não seja regido por qualquer política externa pode publicar uma DPS.

A publicação de uma DPS é mais relevante para entidades que operem uma zona que contém um número significativo de delegações, como um TLD. A publicação de uma DPS ajuda a proporcionar um nível de transparência que aumenta a confiança da comunidade nas operações do TLD. Contudo, como já referido, uma DPS não deve conter informações operacionais sensíveis.

O RFC 6841, *A Framework for DNSSEC Policies and DNSSEC Practice Statements*, é um documento que fornece uma compreensão profunda de uma lista abrangente de tópicos que um operador de TLD deve considerar ao definir uma DP e uma DPS, respetivamente.

3.3.2 Como redigir uma DP e uma DPS

A redação de uma DPS é um passo importante no percurso para assinar um ccTLD. A DPS pode ser curta e simples ou longa e complexa, mas deve ajudar as pessoas a compreenderem a estrutura de operações DNSSEC e como podem confiar no processo de assinatura do ccTLD.

O quadro abaixo resume o conjunto de disposições que consiste em oito componentes delineados no RFC 6841, os quais podem ser considerados aquando da elaboração de uma DP ou DPS. Nem todos os componentes do RFC 6841 são de implementação obrigatória, pelo que o utilizador tem a liberdade de escolher os (sub)componentes adequados às suas

necessidades.

Título	Descrição	Subcomponentes
Introdução	Identifica e introduz o conjunto de disposições e indica os tipos de entidades e aplicações a que se destina a declaração de política ou prática.	● Visão geral ● Nome e identificação do documento ● Comunidade e aplicabilidade ● Administração da especificação
Publicação e Repositórios	Descreve os requisitos para que uma entidade publique informações sobre as suas práticas, chaves públicas e o estado atual dessas chaves, juntamente com pormenores relativos aos repositórios em que as informações são mantidas.	● Repositórios ● Publicação de chaves públicas
Requisitos operacionais	Descreve os requisitos operacionais para o funcionamento de uma zona assinada por DNSSEC.	● O significado dos nomes de domínio ● Identificação e autenticação de um gestor de zona secundária ● Registo de registos de recursos DS ● Métodos para provar a posse e propriedade de uma chave privada ● Remoção de registos de recursos DS
Controlos de Instalações, de Gestão e Operacionais	Descreve os controlos de segurança não técnicos, ou seja, físicos, processuais e de pessoal, para executar com segurança as funções relacionadas com o DNSSEC. Estes controlos incluem o acesso físico, a gestão de chaves, a recuperação de desastres, a auditoria e o ficheiro. Estes controlos de segurança não técnicos são fundamentais para a confiança nas assinaturas geradas pelo DNSSEC.	● Controlos físicos ● Controlos processuais ● Controlos de pessoal ● Procedimentos de registo de auditoria ● Compromisso e recuperação de desastres ● Cessação da entidade
Controlos Técnicos de Segurança	Define as medidas de segurança tomadas para gerir as chaves criptográficas e os dados de ativação, p. ex., números PIN, palavras-passe ou partilhas de chaves detidas manualmente, relevantes para as operações DNSSEC.	● Geração e instalação de pares de chaves ● Proteção de chaves privadas e controlos de engenharia de módulos criptográficos ● Dados de ativação

Assinatura de Zonas	Abrange todos os aspetos da assinatura de zona, incluindo a especificação criptográfica que envolve as chaves de assinatura, o esquema de assinatura, a metodologia para rollover de chaves e a assinatura de zona efetiva.	• Comprimentos de chave, tipos de chave e algoritmos • Negação de existência autenticada • Formato da assinatura • Rollover de chaves • Duração da assinatura e frequência de re-assinatura
	Zonas secundárias e outras partes confiáveis podem depender das informações desta secção para compreender os dados esperados na zona assinada e determinar o seu próprio comportamento.	
Auditoria de Conformidade	Descreve como as auditorias devem ser conduzidas pelo operador da zona e possivelmente por outras entidades envolvidas.	• Frequência de uma auditoria de conformidade da entidade • Identidade/qualificações do auditor • Tópicos abrangidos pela auditoria • Ações pós-auditoria
Questões Jurídicas	Indica em que jurisdição o registry está a ser operado e fornece referências a quaisquer acordos associados que estejam em vigor. A secção “Questões Jurídicas” pode informar sobre quaisquer implicações identificadas na proteção de informações privadas pessoalmente identificáveis.	• Menção da jurisdição aplicável • Obrigações contratuais e cumprimento de leis e regulamentos nacionais, transnacionais ou internacionais • Proteção de dados e tratamento de informações pessoais identificáveis

Podem ser acrescentados componentes adicionais a esta estrutura para responder às necessidades específicas do ccTLD. Para ver exemplos de declarações de práticas DNSSEC, consulte o Anexo A deste guia.

3.3.3 Seleção de algoritmos criptográficos para uma zona

O domínio da criptografia está em constante evolução. Os algoritmos mais recentes substituem os existentes quando se verifica que são menos seguros do que se pensava anteriormente. Por conseguinte, os requisitos de implementação de algoritmos e as orientações de utilização são atualizados regularmente para refletir as novas realidades.

A implementação do DNSSEC requer a escolha de um algoritmo criptográfico adequado. Aquando da publicação deste guia, o RFC 8624, *Algorithm Implementation Requirements and Usage Guidance for DNSSEC*, fornece diretrizes de implementação de algoritmos e requisitos de parâmetros de assinatura relevantes para o DNSSEC.

O quadro seguinte enumera algumas recomendações (não exaustivas) recolhidas do RFC

8624. Os operadores individuais podem ter requisitos específicos e podem querer ajustar-se em conformidade.

Item	Recomendações
Algoritmo DNSKEY	O **algoritmo 13 (ECDSAP256SHA256)** fornece força criptográfica e é atualmente recomendado para utilização em novas implementações DNSSEC devido às suas chaves e tamanho de assinatura mais curtos, resultando em pacotes DNS mais pequenos. Contudo, o **algoritmo 8 (RSASHA256)** também pode ser utilizado, uma vez que está amplamente implementado e é, desde há vários anos, o algoritmo predefinido devido à sua força criptográfica.
Algoritmos Delegation Signer (DS)	O SHA-256 é amplamente utilizado e é um algoritmo de hash forte, pelo que é recomendado para implementações novas e existentes para o DS.
Algoritmo de Segurança DNSSEC (composto pelo algoritmo criptográfico e pelo algoritmo de hash)	A recomendação atual é o algoritmo 13 (ECDSAP256SHA256). Caso contrário, pode também ser utilizado o algoritmo 8 (RSASHA256).
Tamanho da chave da Chave de Assinatura de Zona (ZSK) e da Chave de Assinatura de Chave (KSK)	O algoritmo 13 (ECDSAP256SHA256) irá gerar sempre chaves de 256 bits. A dimensão da chave do algoritmo 8 (RSASHA256) pode ser definida entre 2048 e 4096 bits.
Período de efetividade da ZSK e da KSK	Não existe uma boa forma de estimar as necessidades individuais, uma vez que os operadores ajustam os períodos de validade das chaves com base nas suas experiências anteriores. Vários operadores têm utilizado uma ZSK durante 1-3 meses e uma KSK durante 1-5 anos antes de realizarem um rollover.
Armazenamento de chaves privadas	Máquinas offline, não conectadas à rede e fisicamente seguras, como módulos de segurança de hardware (HSM)

Nota: chaves maiores irão aumentar o tamanho dos registos RRSIG e DNSKEY, aumentando assim a possibilidade de estouro de pacotes UDP do DNS. Para além disso, o tempo necessário para validar e criar assinaturas de registos de recursos (RRSIG) aumenta com chaves maiores, pelo que se deve evitar aumentar desnecessariamente os tamanhos das chaves.

3.3.4 Negação de existência: NSEC ou NSEC3

A negação de existência ou prova de que algo não existe é um mecanismo que informa um resolvedor de que um determinado nome de domínio não existe (NXDOMAIN). Por outro lado, um nome de domínio existe mas não tem o registo de recurso específico (NODATA) que está a ser pedido.
A negação de existência autenticada utiliza criptografia para assinar uma resposta negativa.

No DNSSEC, tal é conseguido utilizando NSEC (Next Secure) ou NSEC3 (Next Secure v3), respetivamente.

O NSEC é utilizado para descrever um intervalo entre nomes. Indica indiretamente a um resolvedor quais os nomes que não existem numa zona, fornecendo, por ordem canónica, o nome que o precede e o nome que o sucede. Este mecanismo implementado no NSEC constitui a base da negação de existência autenticada no DNSSEC e enfrenta dois problemas:

- Os registos NSEC são suscetíveis de zone walking, fraqueza essa que pode permitir a um cibercriminoso percorrer todos os nomes de uma zona. Por conseguinte, é possível reconstruir toda a zona e, assim, anular quaisquer tentativas de bloquear administrativamente as transferências de zona.

- O segundo problema que o NSEC enfrenta numa zona centrada na delegação, como um TLD, é que cada nome nessa zona recebe um registo NSEC e o RRSIG associado. Quando uma zona é assinada, isto leva a um aumento do seu tamanho. As despesas gerais geradas por este aumento podem ter um impacto negativo no desempenho dos servidores DNS autoritativos, como a limitação dos recursos de armazenamento do hardware ou o prolongamento do tempo necessário para efetuar transferências de zona.

Por outro lado, o NSEC3 atenua o problema de zone walking no NSEC, através do hashing dos nomes de domínio com a possibilidade de os endurecer utilizando um recurso de salt. Para além disso, graças a uma funcionalidade específica denominada “opt-out”, os nomes de domínio não assinados delegados numa zona (delegações inseguras) não requerem um registo NSEC3. Isto implica que, quando a funcionalidade “opt-out” é ativada numa zona de TLD, o NSEC3 não pode provar ou negar a existência de domínios não assinados registados nesse TLD. Contudo, um problema apresentado pelo NSEC3 é o facto de as respostas do DNS serem maiores do que as do NSEC.

Não existe uma única resposta adequada quando se trata de escolher entre NSEC e NSEC3. Se alguém preferir usar o NSEC3 para evitar zone walking, a implementação do NSEC3 sem iterações extras e com um salt vazio é geralmente recomendada. Contudo, para zonas mais pequenas, a utilização de registos NSEC3 baseados em opt-out não é recomendada. Para zonas muito grandes e escassamente assinadas, em que a maioria dos registos são delegações inseguras, pode ser utilizada a funcionalidade opt-out do NSEC3. Para além destas considerações, é mais fácil resolver problemas em NSEC do que em NSEC3.

3.4 Envolvimento do registrar

É altamente recomendável envolver os registrars nas fases preliminares da assinatura de um ccTLD. Não só porque são o intermediário entre o registry e os registrants, mas também porque a implementação do DNSSEC ao nível do ccTLD é o ponto de partida para proteger o namespace desse ccTLD. Após assinatura do ccTLD, os titulares de domínios de segundo nível podem começar a proteger os respetivos domínios. Para tal, os registrars têm de ser capazes de recolher e enviar um novo tipo de registo dos titulares de domínios de segundo nível ou de níveis subsequentes para o registry. Este novo tipo de registo é designado por Delegation Signer (DS).

Tecnicamente, o DS é um hash da Chave de Assinatura de Chaves (KSK) e ajuda a estabelecer a cadeia de confiança entre uma zona-mãe e uma zona-filha no espaço de nomes do DNS. A existência do registo DS na zona-mãe cria uma ligação segura que um cibercriminoso externo teria de ultrapassar para forjar material chave na zona-filha.

Por norma, o ccTLD partilha o seu registo DS com a Internet Assigned Numbers Authority (IANA) para publicação na zona raiz. Os registrants e administradores de nomes de domínio sob o ccTLD partilham os seus registos DS com o ccTLD diretamente ou através de um registrar. Os Registrars desempenham aqui dois papéis importantes:

- **Fornecer uma interface ou mecanismo seguro e fiável para recolher registos DS** dos registrants; se essa interface ou mecanismo ainda não existir, os registrars dispostos a oferecer suporte DNSSEC aos seus registrants devem trabalhar o mais rapidamente possível para o implementar. Não existe uma forma normalizada de mover o registo DS entre o cliente e o registrar. Os diferentes registrars têm mecanismos diferentes, que vão desde simples interfaces Web a várias API.
- **Enviar o DS para o registry.** Recomenda-se uma solução automatizada de publicação do DS na zona-mãe em vez de uma intervenção manual. No modelo registry-registrar, é possível utilizar as extensões DNSSEC ao EPP para a transferência de conjuntos de registos de recursos (RRsets) DS e, opcionalmente, DNSKEY RRset. Em qualquer caso, devem ser realizados testes entre o operador de ccTLD e os registrars para garantir que as novas transações são viáveis utilizando a infraestrutura existente.

Outro mecanismo para a zona-filha gerir automaticamente o DS com a entidade-mãe é utilizar um CDS (Child DS) ou um RRset CDNSKEY (Child DNSKEY) se a entidade-mãe tiver uma política de aceitação destes registos. Podem ser utilizados nas três seguintes situações:

- Publicação inicial de DS;
- Rollover de chave;
- Regresso ao estado inseguro.

De forma simples, o CDS/CDNSKEY é uma instrução para a entidade-mãe modificar o RRset do recurso DS se o CDS/CDNSKEY e o DS forem diferentes. O RFC 8078, *Managing DS Records from the Parent via CDS/CDNSKey*, explica de forma pormenorizada a gestão automatizada dos registos DS entre as zonas filha e mãe.

Por fim, o envolvimento dos registrars no início do processo também permite que estes beneficiem de formação em DNSSEC e dos programas práticos oferecidos pela ICANN e respetivos parceiros na comunidade da Internet.

4 Cronograma

Não existem prazos específicos para a implementação do DNSSEC. A duração pode variar entre algumas semanas até meses ou anos, dependendo de vários fatores. Contudo, devem-se considerar as seguintes sugestões para evitar grandes atrasos:

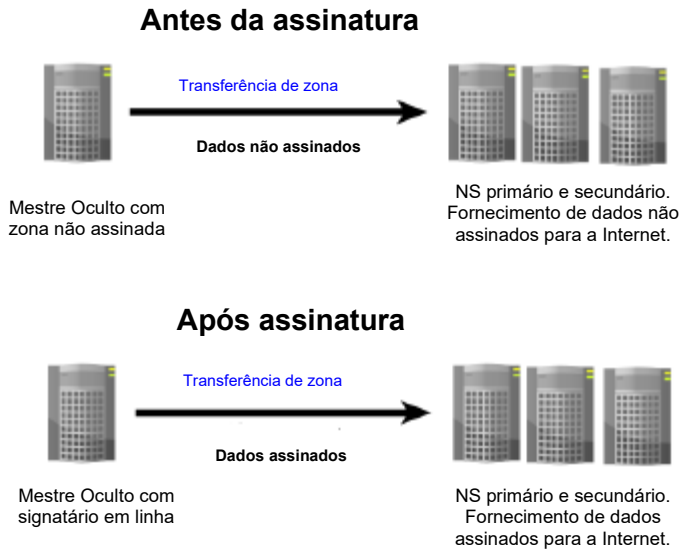
- Definir o processo como um projeto com uma data de início clara, uma data de fim prevista e marcos a atingir. Para além disso, deve atribuir um gestor de projeto ou um responsável técnico com os recursos adequados;
- Definir, gerir e colaborar com as partes interessadas, incluindo, entre outras, a(s) entidade(s) reguladora(s), o(s) registrar(a), as partes técnicas e administrativas, os contratantes, o(s) operador(es) de backend ou qualquer outra parte. É igualmente necessário abordar a comunicação entre as diferentes partes interessadas nos ccTLD's.
- Identificar e gerir corretamente os riscos

5 Cenários de implementação do DNSSEC

Quer decida gerir a zona utilizando apenas os seus próprios recursos e infraestruturas ou através da contratação de um prestador de serviços, como um operador de backend, é provável que a arquitetura de implementação técnica siga um dos dois cenários principais aqui descritos.

5.1 Servidor primário para assinatura em linha (primário oculto)

Neste cenário de configuração, um servidor de nomes primário oculto, normalmente desconhecido da Internet, serve a zona para um conjunto de servidores DNS autoritativos, normalmente para um servidor primário público e para vários servidores secundários. Um servidor de nomes primário oculto não é um requisito específico do DNSSEC, mas antes uma prática recomendada de funcionamento do DNS que sugere a existência de um servidor de nomes autoritativo fora da banda, inacessível e desconhecido do público e onde podem ser efetuadas todas as atualizações de zona. Este servidor deve também implementar procedimentos de segurança e auditoria mais rigorosos. A arquitetura assemelha-se à figura abaixo:

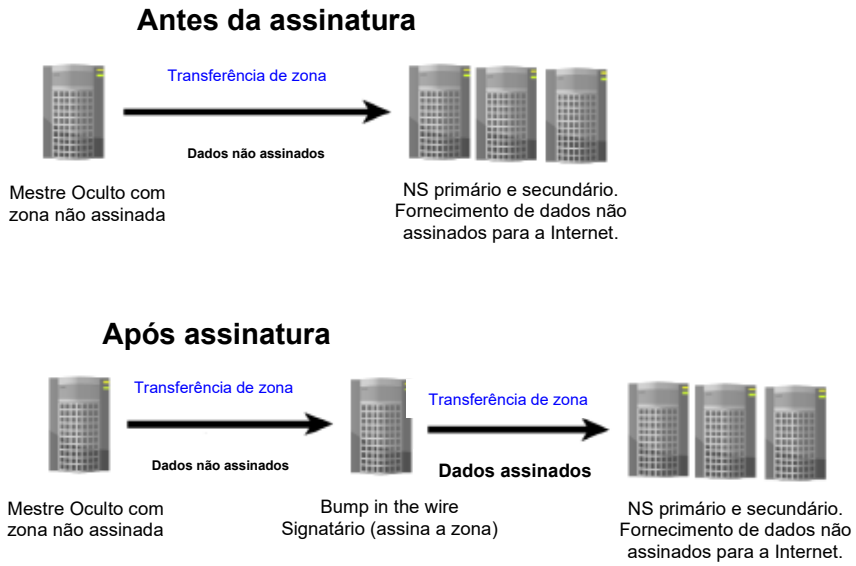


Este servidor primário oculto será configurado para reconhecer as chaves criadas e usá-las para gerar e executar uma zona assinada, seguindo o processo fornecido pelo software DNS que executa. Após conclusão, a versão assinada do ficheiro de zona será transferida e mantida sincronizada com todos os servidores de nomes autoritativos publicamente visíveis adequados.

Salvo em relação às alterações de configuração no servidor de nomes primário oculto, não existem outras alterações adicionais de configuração ou de software a efetuar nesta arquitetura.

5.2 Assinatura em linha “bump-in-the-wire”

Neste cenário de configuração, um novo servidor de nomes, o signatário, é inserido na arquitetura existente e colocado entre o servidor primário oculto e os servidores de nomes públicos que servem a zona na Internet. Este novo servidor age como um dispositivo bump-in-the-wire (BITW). Recebe o ficheiro de zona não assinado do primário oculto, assina os dados e envia o ficheiro de zona assinada para ser distribuído aos servidores de nomes públicos do domínio.



Para o conseguir, devem-se considerar os seguintes passos:

1. O servidor primário oculto não deve ser listado no RRset de recursos do servidor de nomes (NS) para o domínio, para evitar respostas contraditórias, ou seja, respostas não assinadas do servidor primário oculto e respostas assinadas de outros servidores de nomes.
2. A configuração do servidor primário oculto deve ser atualizada para permitir que apenas o signatário realize uma transferência de zona.
3. O signatário utiliza o ficheiro de zona não assinado recebido do servidor primário oculto e uma chave privada para assinar os registos de recursos. Por fim, distribui o ficheiro de zona assinada pelos servidores de nomes primários e secundários utilizando mecanismos de transferência de zona.
4. A configuração dos servidores de nomes também deve ser atualizada em conformidade para receber a transferência de zona apenas do signatário.

Independentemente do cenário de implementação, é aconselhável verificar a zona assinada antes de a distribuir por todos os servidores. Este exercício de verificação pode ser realizado no nome de domínio, utilizando ferramentas online, como as descritas na secção 10 deste documento. É igualmente boa prática executar várias consultas à procura de assinaturas de registos de recursos DNSSEC e datas de expiração de assinaturas, entre outros parâmetros em cada uma das zonas a ser administradas. Inclua estas execuções de teste como parte da validação da sua implementação.

Em resumo, vamos comparar as etapas da cadeia de produção de zonas entre o DNS normal e o DNSSEC:

- **DNS normal:** Criar → Validar → Publicar → Monitorizar
- **Com DNSSEC:** Criar → Validar → Assinar → Validar → Publicar → Monitorizar

6 Assinar um TLD

Tal como com qualquer outra alteração importante, é fortemente aconselhável realizar uma fase de testes aprofundados antes de planear uma implementação no sistema de produção. É ainda mais necessário no caso do DNSSEC, porque são introduzidas novas alterações na zona. Os passos abaixo descritos fornecem uma visão geral para assinar uma zona TLD; com base no seu ambiente e requisitos específicos, poderá ser necessário ajustá-los.

Em alguns casos, assinar todo o ficheiro da zona de uma só vez seria inadequado para grandes ccTLD's; em vez disso, seria mais seguro estabelecer uma abordagem incremental para assinar a zona. Outros ccTLD's também podem optar por assinar primeiro uma zona secundária num banco de ensaio, antes de adicionar um registo DS à zona-mãe. Trata-se de um teste preparatório antes da assinatura da zona ccTLD efetiva.

Em qualquer caso, para concluir com êxito o processo de assinatura, seria sensato proceder com cautela, adotando planos de implementação e teste adequados, acompanhados de uma metodologia de validação rigorosa.

1. Implementar e configurar um ambiente de teste DNSSEC. Dependendo do modelo de implementação, o banco de testes pode conter os seguintes elementos:
   - Um servidor de assinatura de teste, um servidor de nomes (NS de teste), capaz de assinar um ficheiro de zona; O servidor deve poder gerar as chaves de assinatura ou receber chaves geradas por um servidor diferente ou por um módulo de segurança de hardware (HSM), assinar a zona e distribuir o ficheiro de zona assinada, entre outras funções.
   - Um servidor de nomes autoritativo secundário de teste irá receber a zona assinada e servi-la-á.
   - Um resolvedor de teste deve ser configurado para executar validações DNSSEC localmente para a zona assinada.
2. Copiar o ficheiro de zona não assinado do servidor primário oculto para o servidor de assinatura de teste. A distribuição do ficheiro de zona não assinada para o sistema de assinatura de teste pode ser automatizada mais tarde na fase de teste.
3. Gerar as chaves KSK e ZSK. Recomenda-se a geração de chaves fora do sistema de assinatura. Armazenar a KSK num HSM ou offline e utilize-a apenas para assinar os registos de recursos DNSKEY.
4. Assinar a zona e publica-la no(s) servidor(es) de nome(s) secundário(s) de teste.
5. Gerar e importar o DS como chaves de confiança para o resolvedor de teste. No mundo real, o DS não será distribuído aos resolvedores recursivos de todo o mundo diretamente pelos administradores do TLD; em vez disso, será enviado à IANA para publicação na zona raiz. Qualquer resolvedor recursivo validado em todo o mundo irá buscar à zona raiz o DS correspondente a esse TLD.
6. Executar alguns testes através da realização de Testes de Aceitação do Utilizador (UAT) com base em casos de teste definidos. Os testes devem abranger tópicos como a recuperação das chaves e assinaturas, a verificação da expiração das assinaturas, o tempo de resposta da consulta e o tamanho. Efetuar a validação DNSSEC, entre outras tarefas.
7. Se o processo de assinatura de teste for automatizado, observar a expiração da

assinatura e a geração automática de novas assinaturas. Caso contrário, deve executar rollovers manuais até que o processo de assinatura de teste esteja automatizado.

8. Realizar o rollover da ZSK e o rollover da KSK. Para um rollover KSK, gerar o novo DS e simular a partilha com a zona-mãe, adicionando-o ao resolvedor de teste para validação local. Dependendo de vários parâmetros de tempo, como o período de validade da chave no ambiente de teste, será necessário remover o DS antigo do resolvedor de teste e a KSK antiga da zona para concluir o rollover da KSK.
9. Efetuar novos testes iterativamente e aperfeiçoar os passos 1 a 8.
10. Quando estiver confiante com a metodologia de teste, concentrar-se no go live e escolher o ambiente apropriado e o cenário de implementação da sua preferência: BITW ou assinatura primária oculta em linha. Realizar um novo UAT para confirmar que todos os servidores de nomes autoritativos do domínio servem corretamente a zona e os registos de recursos DNSSEC correspondentes.
11. Por fim, publicar o DS na zona raiz seguindo as diretrizes de gestão de delegações para TLD, conforme definido pela IANA em https://www.iana.org/domains/root/manage. Uma vez adicionado à zona raiz, anunciar ao mundo que o ccTLD é assinado por DNSSEC e que qualquer resolvedor com preocupações de segurança deve efetuar a validação DNSSEC dos registos DNS provenientes dessa zona. Recomenda-se vivamente a utilização de uma ferramenta como a https://dnsviz.net/ (ver Secção 10 para mais informações) para validar a cadeia de confiança DNSSEC para a zona.
12. Quando o ccTLD estiver “oficialmente assinado”, planear abrir o acesso para que os registrars publiquem os registos DS dos registrants no registry para que a cadeia de confiança fique efetiva.

7 Rollover de chaves e algoritmos

Quando uma zona é protegida com DNSSEC, o gestor de zona tem de estar preparado para substituir (ou “rollover”) as chaves utilizadas para proteger a zona, quer seja periodicamente por questões de segurança ou operacionais ou em caso de emergência. Para implementar um rollover de chave ou de algoritmo, é necessário introduzir novas chaves e eliminar da zona as chaves antigas. É fundamental ter em conta que os dados publicados para uma zona residem em várias caches de resolvedores. Ignorar os dados que podem estar em caches pode levar à perda de serviço para os clientes. Por exemplo, considere os dados da zona assinados com uma chave antiga, que está a ser validada por um resolvedor que não tem a chave da zona antiga na sua cache. Se a chave antiga já não estiver presente na zona atual, a validação irá falhar e os dados da zona correspondente serão marcados como falsos.

Por outro lado, um resolvedor que tente validar dados assinados com uma nova chave, enquanto a chave antiga ainda se encontra na cache do resolvedor, também resulta na marcação dos dados como falsos. Existem vários tipos de técnicas de rollover de chaves e algoritmos, como as descritas no RFC 6781, *DNSSEC Operational Practices, Version 2* assim como no RFC 7583, *DNSSEC Key Rollover Timing Considerations*. Exemplos dessas técnicas são a *pré-publicação*, o *rollover da ZSK duplo RRSIG, o duplo da KSK, o duplo DS e o duplo RRset*, para indicar algumas.

No caso específico em que é necessário um rollover de chave de emergência porque se suspeita que um par de chaves ZSK ou KSK esteja comprometido, é aconselhável já ter um procedimento documentado em vigor.

7.1 Rollover da ZSK

Durante um rollover da ZSK, é essencial garantir que qualquer validador de cache que tenha

acesso a uma determinada assinatura também tenha acesso à ZSK válida correspondente. O RFC 6781, *DNSSEC Operational Practices, Version 2* documenta três métodos para efetuar um rollover da ZSK: pré-publicação, assinatura dupla e duplo RRSIG.

Neste documento, descreveremos apenas o método de pré-publicação, uma vez que mantém os tamanhos da zona e da resposta a um nível mínimo durante todo o processo de rollover. Neste método, a nova ZSK é introduzida no DNSKEY RRset e depois de decorrido tempo suficiente para garantir que quaisquer DNSKEY RRset em cache contêm ambas as chaves. A zona é depois assinada utilizando a nova ZSK e as assinaturas antigas são removidas. Por fim, quando todas as assinaturas criadas com a ZSK antiga tiverem expirado das caches, a chave antiga é removida. Os passos abaixo descrevem o processo.

1. A nova ZSK A é introduzida na zona e aparece no DNSKEY RRset, não sendo ainda utilizada para assinar registos na zona. As KSK atualmente ativas renunciam ao DNSKEY RRset, que é então assinado novamente com as KSK atualmente ativas. Nesta fase, diz-se que a nova ZSK está publicada.
2. Após um determinado período de tempo, a ZSK A fica pronta para assinar registos na zona. Este período corresponde ao atraso de propagação da zona mais o tempo de vida dos registos DNSKEY na zona. Por outras palavras, é o tempo máximo necessário para que os registos DNSKEY existentes expirem das caches. A ZSK A torna-se ativa e começa efetivamente a assinar registos para a zona.
3. A ZSK A irá continuar a assinar e a atualizar registos para a zona até que seja necessário publicar uma nova ZSK B. O tempo de publicação da chave B depende do tempo de ativação de A e do tempo de vida da ZSK definido para a zona na política de gestão de chaves. A ZSK B fica pronta e pode ser utilizada para assinar registos, mas a ZSK A ainda está ativa.
4. Quando o tempo de vida da ZSK é atingido para a chave A, esta é retirada. A chave B torna-se ativa e é utilizada para assinar a zona. Contudo, a chave retirada deve ser mantida na zona durante algum tempo (para um “intervalo de retirada”) para permitir que o RRSIG seja gerado utilizando essa chave para continuar a ser validado pelos resolvedores. O intervalo de retirada corresponde ao tempo necessário para que todos os RRsets existentes sejam novamente assinados com a chave B, mais o atraso de propagação da zona e o TTL máximo de todos os RRSIG criados com a chave antiga na zona.
5. Após um determinado período de tempo, as assinaturas criadas com a chave retirada desaparecem das caches dos resolvedores e a chave antiga é considerada morta.
6. Quando a chave antiga está morta, esta pode ser removida do conjunto DNSKEY RRset, que deve ser assinado novamente com as KSK da zona atual. Nesta fase, a chave A é declarada removida.
7. Após algum tempo, uma nova chave será publicada e todo o processo será repetido.

7.2 Rollover da KSK

Num rollover de KSK, o principal desafio consiste em garantir que existe sempre uma KSK de confiança para a zona, mesmo durante o processo de rollover. O RFC 6781, *DNSSEC Operational Practices, Version 2* também documenta três métodos de rollover de uma KSK: double-KSK, double-DS e double-RRset. O método Double-RRset é o mais eficiente destes métodos, uma vez que tanto os novos registos DS como os DNSKEY RRsets se propagam em paralelo.

Com este método, os novos registos DNSKEY e DS são publicados simultaneamente nas zonas apropriadas. Depois de decorrido tempo suficiente para que os antigos RRsets DNSKEY e DS expirem das caches, são removidos das respetivas zonas. As etapas de rollover encontram-se descritas a seguir:

1. Os registos DS e DNSKEY estão presentes nas respetivas zonas. A sua KSK A

correspondente está ativa e a proteger a zona.

2. Quando o tempo de vida da KSK A atual se aproxima, uma nova KSK B é introduzida na zona e utilizada para assinar o DNSKEY RRset. O DS da KSK B é enviado à entidade-mãe para publicação na zona-mãe.
3. A entidade-mãe pode proceder à verificação do novo DS e depois publicá-lo na zona-mãe.
4. Após um período de tempo, o novo DS ou DNSKEY já se propagou para as caches dos resolvedores de validação. Ao mesmo tempo, a ZSK A é removida da zona.
5. Mais tarde, os registos DS e DNSKEY associados à ZSK A são também removidos.
6. Após algum tempo, uma nova chave será publicada e todo o processo será repetido.

8 Outras considerações para zonas assinadas

Vale a pena considerar os seguintes elementos na preparação de uma estratégia de implementação de DNSSEC:

- **Definir um programa de desenvolvimento de capacidades:** Identificar e participar em workshops, webinars, formação prática e quaisquer outras atividades de capacitação que possam ajudar a aumentar os conhecimentos e a desenvolver novas competências nas operações do DNSSEC. O Compromisso Técnico da ICANN ministra essas formações, incluindo seminários sobre DNSSEC, normalmente realizadas durante as reuniões da ICANN.
  - Para além da ICANN, o Network Startup Resource Center (NSRC), a Internet Society e os Registries Regionais da Internet (RIR) também disponibilizam atividades de envolvimento relacionadas com o DNSSEC.
  - Por último, a participação em fóruns, webinars e workshops em que operadores experientes e recém-chegados se reúnem, apresentam e discutem implementações atuais e futuras do DNSSEC pode aumentar consideravelmente o seu conhecimento das práticas operacionais do DNSSEC.
- **Subscrever as listas de correio eletrónico do NOG:** Estes são bons fóruns onde as pessoas discutem e partilham as suas experiências e conhecimentos técnicos, bem como procuram apoio e assistência em questões técnicas. Pense nelas como uma comunidade que o pode ajudar quando necessário.
- **Gerar e gerir chaves:** Os módulos de segurança de hardware (HSM) tendem a fornecer uma boa facilidade para gerar e armazenar chaves privadas. Contudo, vale a pena considerar os custos de compra, segurança e manutenção do HSM. Dependendo das suas caraterísticas, os custos dos HSM podem variar de algumas centenas a milhares de dólares. Os HSM também podem aumentar as despesas de formação, uma vez que a aprendizagem de qualquer novo hardware tem os seus desafios. A utilização de HSM é uma boa prática, mas não é o único método de geração de chaves. Outra possibilidade que vale a pena considerar é gerar, armazenar e utilizar as chaves privadas numa máquina off-line, sem ligação à rede e fisicamente segura. O RFC 6781, *DNSSEC Operational Practices, Version 2* fornece mais pormenores sobre a geração e gestão de chaves.
- **Considerações sobre o tempo:** O DNSSEC introduz a noção de tempo absoluto no DNS. No DNSSEC, as assinaturas têm um período de validade desde a sua data de início até à sua data de expiração, após a qual a assinatura é marcada como inválida e os dados assinados são considerados falsos. É fundamental garantir que o tempo é bem gerido para que as assinaturas sejam geradas com o período de validade correto. Imagine uma zona assinada cujo período de validade da assinatura já foi ultrapassado; isso ira resultar numa falha de validação no final do resolvedor. Assim, recomenda-se

vivamente a configuração do servidor Network Time Protocol (NTP) para manter a hora exata. Há ainda outras considerações, como o tempo mínimo e máximo de vida da zona (TTL), o período de publicação da assinatura e o período de validade da assinatura, conforme descrito no RFC 6781, *DNSSEC Operational Practices, Version 2*.

- **Requisitos de software, hardware e rede:** Tanto as implementações de DNSSEC de código aberto como as comerciais são atualmente suportadas, incluindo o Berkeley Internet Name Domain (BIND), o PowerDNS, o NLnet Labs Name Server Daemon (NSD) e o Knot DNS, para citar alguns. O OpenDNSSEC é uma solução de assinatura que continua a ser amplamente utilizada, uma vez que automatiza o processo de controlo das chaves DNSSEC e a assinatura de zonas. Se deseja implementar o DNSSEC num servidor autoritativo, terá de gerar as chaves de assinatura criptográficas no sistema. A quantidade de tempo necessária para gerar as chaves depende da fonte de aleatoriedade (entropia) no sistema. Sistemas como máquinas virtuais com entropia insuficiente podem demorar muito mais tempo a gerar chaves.
  - Os recursos de hardware, como a CPU, o armazenamento do sistema e a memória, também são áreas que vale a pena considerar para possíveis otimizações. Tal ocorre porque a ativação do DNSSEC aumenta o armazenamento do sistema, a utilização da memória e a carga da CPU, em parte devido à geração e assinatura de chaves. Uma zona assinada é sempre acompanhada por um aumento considerável no ficheiro de zona.
  - Em relação às políticas de segurança de rede, verifique se as regras de firewall e ACL, p. ex., permitem pacotes DNS UDP grandes e DNS sobre TCP na porta 53. Para além disso, o Mecanismo de Extensão para DNS (EDNS0) tem de ser ativado nos servidores DNS e na configuração da rede, respetivamente.

9 Cancelamento da assinatura do TLD, se necessário

O DNSSEC, como muitas coisas neste mundo, não está isento de problemas. Quando se acrescenta mais complexidade ao DNS, aumenta a probabilidade de as coisas se avariarem ou correrem mal. Por exemplo, a KSK ou a ZSK, ou ambas, podem perder-se ou ficar comprometidas. Um erro imprevisto de hardware ou software pode impedir que uma zona seja assinada e distribuída, afetando assim o serviço adequado de uma zona.

Na pior das hipóteses, pode preferir cancelar a assinatura da zona para corrigir quaisquer problemas e erros antes de assinar novamente. Contudo, cancelar a assinatura de um domínio implica o custo de o reverter para um estado inseguro.

O mundo sabe se uma zona está assinada ou não assinada pela presença de um registo DS na zona-mãe. Se não existir nenhum registo DS, a cadeia de confiança não está assegurada. Por conseguinte, reverter para um estado não assinado é tecnicamente tão fácil como remover todos os registos DS da zona-mãe. No caso de um ccTLD, isto implica solicitar à IANA que remova o(s) registo(s) DS correspondente(s) da zona raiz.

Após a resolução de todos os problemas, o operador do TLD deve considerar a possibilidade de gerar novas chaves e assinar novamente a zona. Para além disso, o operador deve certificar-se de que a zona recém-assinada está bem distribuída e disponível em todos os servidores de nomes antes de publicar um novo registo DS na zona raiz.
Quando o DS é publicado pela IANA, toda a Internet fica a saber que a zona TLD foi novamente assinada e que qualquer resolvedor de validação irá verificar todos os registos de recursos servidos por essa zona.

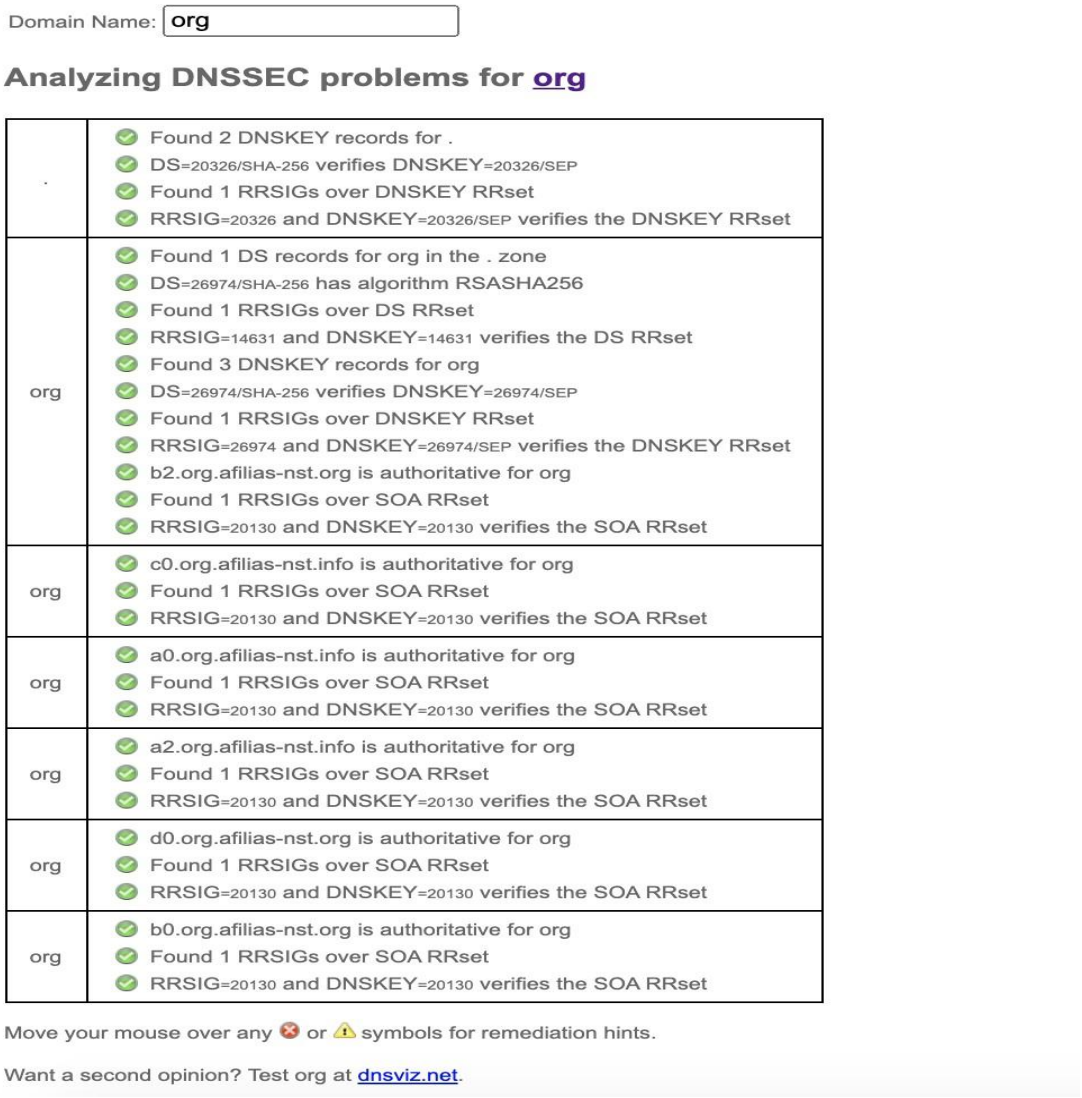
10 Ferramentas DNSSEC úteis

As seguintes ferramentas podem ser úteis para solucionar problemas de DNSSEC.

10.1 Depurador DNSSEC da Verisign

Este depurador DNSSEC, disponível em https://dnssec-debugger.verisignlabs.com/, é uma ferramenta baseada na Web que ajuda a garantir que a "*cadeia de confiança*" está intacta para um determinado nome de domínio com DNSSEC. Apresenta uma validação passo a passo de um determinado nome de domínio e destaca quaisquer problemas encontrados.

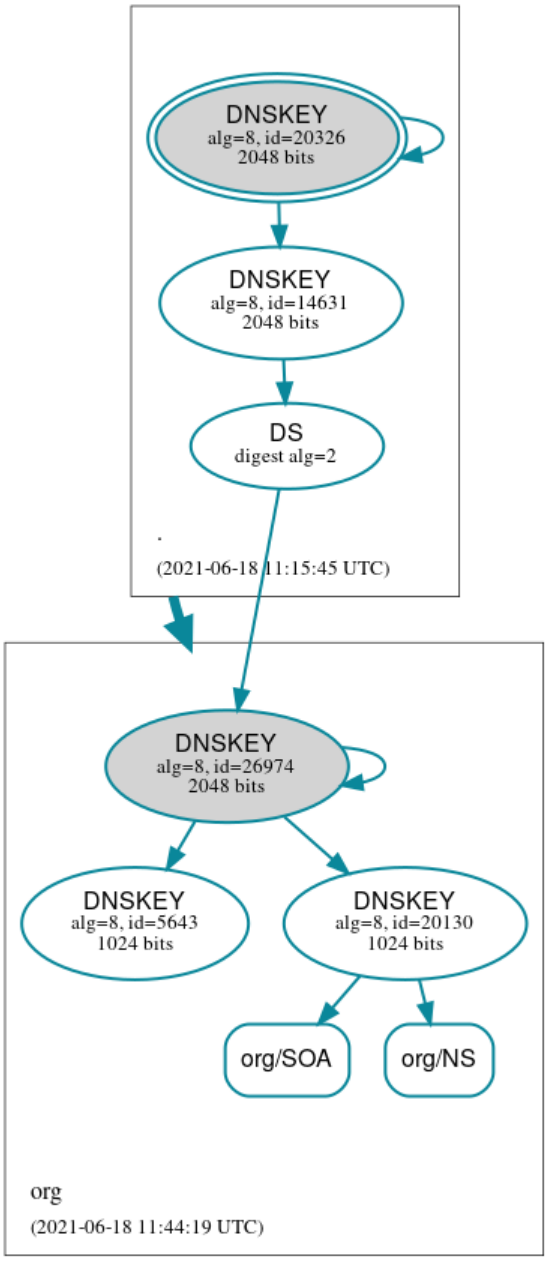
Abaixo encontra-se um exemplo do resultado:



10.2 DNSVIZ

O DNSViz (https://dnsviz.net) é uma ferramenta para visualizar o estado de uma zona DNS. Fornece uma análise visual da cadeia de autenticação DNSSEC para um nome de domínio e o

seu caminho de resolução no namespace DNS. Também lista os erros de configuração detetados pela ferramenta. Abaixo encontra-se uma visualização da zona .ORG:



11 Conclusão

O DNSSEC é um protocolo robusto que fornece autenticação e integridade dos dados do DNS. A assinatura de um nome de domínio com DNSSEC altera muitas questões a nível operacional, introduzindo novos conceitos e tarefas que não existiam com o DNS normal.

Este documento é um guia para ajudar os operadores de registry ccTLD e qualquer outra parte a compreender o que constitui a assinatura de um ccTLD. Há muito que discorrer sobre o DNSSEC e este documento abrangeu alguns dos aspetos mais importantes de uma implementação.

Tal como qualquer outra solução de segurança, é aconselhável seguir um processo adequado e preparar-se para evitar quebras. Todas as partes devem avaliar o seu próprio ambiente e as ameaças e vulnerabilidades associadas para determinar o nível de risco que estão dispostas a aceitar quando confiam no DNSSEC para proteger a sua zona e os domínios nela contidos.

Essencialmente, os esforços coordenados e a colaboração ativa de todas as partes interessadas continuam a ser fundamentais para a implementação bem sucedida do DNSSEC.

A Exemplo de Políticas DNSSEC e Declaração de Práticas DNSSEC

- ZACR DNSSEC Policy and Practice Statement Framework, version 001, set. 2016, ZACR: https://www.registry.net.za/downloads/u/zacr-dps-signed.pdf
- DNSSEC Practice Statement .fr, version 1.2, jun. 2013, Afnic: https://www.afnic.fr/wp-media/uploads/2020/12/dps-english-fr.pdf
- CIRA DNSSEC Practice Statement for .CA, version 1.5, ago. 2016, CIRA: https://www.cira.ca/cira-dnssec-practice-statement-ca
- DNSSEC Practice Statement for the JP Zone (JP DPS), version 1.4, out. 2015, JPRS: https://jprs.jp/doc/dnssec/jp-dps-eng.v1.4.html
- Verisign DNSSEC Practice Statement for TLD/GTLD Zone, version 1.8, dez. 2019, Verisign Inc.: https://www.verisign.com/assets/20191111_CTLD_VerisignDNSSECPracticeStatement_v1.8_finalized.pdf. A lista de zonas aplicáveis pode ser consultada em https://www.verisign.com/assets/20190430-Verisign-Operated-TLD-GTLD-Zones-v1.04-Converted.pdf

B Exemplo de zona não assinada e de zona assinada

B.1 Zona não assinada

```
example.                        86400 IN      SOA     a.nic.dns.blablabla.
hostmaster.dns.blablabla. (
                  2017072300 ; serial
                  1800         ; refresh (30 minutes)
                  900          ; retry (15 minutes)
                  2419200      ; expire (4 weeks)
                  300          ; minimum (5 minutes)
                  )

example.                        86400  IN      NS    a.nic.dns.blablabla.
example.                        86400  IN      NS    b.nic.dns.blablabla.
example.                        86400  IN      NS    d.nic.dns.blablabla.
example.                        86400  IN      NS    e.nic.dns.blablabla.
example.                        86400  IN      NS    f.nic.dns.blablabla.
aaa.example.                    86400  IN      NS    ns1.reg.zzzz.
aaa.example.                    86400  IN      NS    ns2.reg.zzzz.
```

```
bbb.example.                    86400 IN      NS    ns1.reg.zzzz.
bbb.example.                    86400 IN      NS    ns2.reg.zzzz.
ccc.example.                    86400 IN      NS    ns1.reg.zzzz.
ccc.example.                    86400 IN      NS    ns2.reg.zzzz.
ddd.example.                    86400 IN      NS    ns3-12.nic.zzzz.
```

B.2 Zona assinada

```
example.                    86400 IN      SOA    a.nic.dns.blablabla.
hostmaster.dns.blablabla. (
                2017072305 ; serial
                1800       ; refresh (30 minutes)
                900        ; retry (15 minutes)
                2419200    ; expire (4 weeks)
                300        ; minimum (5 minutes)
                )

example.                    86400 IN      RRSIG SOA 8 1 86400 20170724231821
20170618015310 660 example. nQ8H8StSRDoQgzwBNQ0k9+E1LGrV0tsCinoB6KxcyuHfGT4ehWsj5JI6
N01WpXqy/q1S/XlhqtjVoiti4zSOwIjFlSloug3W09eJnH9biwmb6U8B
JQoHf3edGvZtWNZdtcOKY1CFBI2ApceFn8KOYvT0qzpygOlF5lMrJvnO J5c=
example.                    86400  IN     NS     a.nic.dns.blablabla.
example.                    86400  IN     NS     b.nic.dns.blablabla.
example.                    86400  IN     NS     d.nic.dns.blablabla.
example.                    86400  IN     NS     e.nic.dns.blablabla.
example.                    86400  IN     NS     f.nic.dns.blablabla.
example.                    86400  IN     RRSIG  NS 8 1 86400 20170730192856
20170617025305 660 example. KNaF2jTPuCGq5FIzspbJL+TDBx/6z01E7+tkkzYRNh0xAKDnutcfb1It
D7XrNWPEbXsaafFyZ/M5DaDGzTzsVNm1h9h3md6o0vZNH07q8nmm+fYX
do8sx9aFxCgl9NsmG0cyrBbVnyrPKxDlAx69HJCh0kBb7PFKhr1hpnYY xGA=
example.                    86400 IN      DNSKEY 256 3 8
AwEAAasHjitdDurpevNLojD4Sp3609P+C9uOTR42DJel0NSSva/x38Ba
7gs0b4Q+tmKPI5cmxDhECiUfdzaRRA8vxPZK8x5LL/V1WZ5q6egFmH4x
eLxWaxlftFotev/T8kVe7jZUk7Hh3x7LPgGLajpjNNFELj42Xe6XBkkN 9FY1lQkB
example.                    86400 IN      DNSKEY 257 3 8
AwEAAY6HLDY5M5kjlrjVV9HQyWUkkrYZ2eB8KeJjUMN9qDM6FsA57pbS
5tmbGV1zxxqGon0pO7HYV06GZIgFOLBqDvgGsnKDQ5A2iktYNuSmTh+w
fd8ixgbYigtoBMBnNeqFozMK58c1yf7amui2cCOg9ibGZMpLQvjKOSyV
Jnlh0l8e3OE7Ul1GEa39XpVez2wkjImhsG0e7KAZPlFjEUpvwie8HEQV
jz3PK7Zr6SZVLLyet0rnN3prCHfvhNh6DycN/rt6/PopLvPQM8SaW+u8
zn6Z4S4AoTPTxKm5udzb7mWf7lT83PAbOvLu/WIRY6nqye+4SkJsrmjI xnLdk/Q54E8=
example.                    86400 IN      RRSIG DNSKEY 8 1 86400 20170703000000
20170613000000 54322 example. B2riGYos+/q5RqXVBQKrrkVUuruDBH8ANNa8J6sMHUjf0MPZOuICd2kZ
PlAGMpZpp8LoaRoG2zaTVILZ8Vhi90FsyLsZVpPooAvmKlTFOrWoJoPo
XScLhb3ISRLOzKEnyLt5Ds3TxuabHLPlf8jpTXaHMFZCzYYtTJJQb+M3
BLeK+Lx4uCwU1pvxNkuR9StKa5tJquByIZCWZsSx5nKWPyrsGLtFJKrg
DXe8XlA8LxeER69OQgSZ1VXvK8Kd4p3wyvzUHCcsPYZzebxHXPqDrYB7
BU7eqsDUjCfThqbkC0Ju7koHROYRjGdoY/4f6nDOJEOICIFEgEDHJg2t w1nENQ==
example.                    0      IN     NSEC3PARAM 1 0 3 00FF
example.                    0      IN     RRSIG NSEC3PARAM 8 1 0 20170716213640
20170606005304 660 example. a6Mp1NjW2/nnn+5i98AWzVrOX0yUvu/urP1cqY6zZjISReZOSLx6aorJ
lM9Nnx1fNVr2COtD71UVJI7kFUC5jVbmAitWdHHH/zyzK6WyyaN5Nsaf
cKW0Su8lLkctCHiqpKmuhOhnK1Dqmigx8YhyhPbN5nCzoST6lcnNjtV0 TwQ=
aaa.example.          86400 IN     NS     ns1.reg.zzzz.
aaa.example.          86400 IN     NS     ns2.reg.zzzz.
```

```
bbb.example.        86400  IN     NS     ns1.reg.zzzz.
bbb.example.        86400  IN     NS     ns2.reg.zzzz.
ccc.example.        86400  IN     NS     ns1.reg.zzzz.
ccc.example.        86400  IN     NS     ns2.reg.zzzz.
ddd.example.        86400  IN     NS     ns3-l2.nic.zzzz.
0KPQJ71AL5RHRST9HM8LEFLK0I0QN5N7.example.      3600 IN      NSEC3 1 1 3 00FF
464L7A368JEOCPKU9G34B9RQADEPKA14 NS DS RRSIG
0KPQJ71AL5RHRST9HM8LEFLK0I0QN5N7.example.      3600 IN      RRSIG NSEC3 8 2 3600
20170703210235 20170602012306 660 example.
H+qdaHqnAgUa66VSKmMmfKWopeZQM0ridMUN2YN4rncHeWD8b0yA6O6N
hLF/ojpZoGrQN+G+p4SWJVb/pj2CkLk00E2AhloXXV0KaQIzUwPVNm7p
J9es7ohi5ErGtM1ClLpGggz05qNWboejbrXtS8TFdoTtn6Z2Omk4RNmj hG0=
464L7A368JEOCPKU9G34B9RQADEPKA14.example.      3600 IN      NSEC3 1 1 3 00FF
MLTMB5J4Q7T5R3GJBSBTMVD2LBMFU3KA NS DS RRSIG
464L7A368JEOCPKU9G34B9RQADEPKA14.example.      3600 IN      RRSIG NSEC3 8 2 3600
20170715005821 20170610062309 660 example.
dk6WScB3zmJYig0w8LxFXoc9vj1leqFRBlET4YAVVmeAwcGf0ixa41T+
pKKcMHbXDsw+PHYZHaRLmA9lEgs+4lJMdA3fRroNSXyV2usHMdFaKUoG
UZKehVGdgrBRx4vx+o4w1ztdumY6MsD0ART6IrhUbr+cvGHAlxNSviCI BbE=
MLTMB5J4Q7T5R3GJBSBTMVD2LBMFU3KA.example.      3600 IN      NSEC3 1 1 3 00FF
0KPQJ71AL5RHRST9HM8LEFLK0I0QN5N7 NS SOA RRSIG DNSKEY NSEC3PARAM
MLTMB5J4Q7T5R3GJBSBTMVD2LBMFU3KA.example.      3600 IN      RRSIG NSEC3 8 2 3600
20170706043605 20170604225320 660 example.
Ndq6p+Y8ztlgNN1vH12o5rxxh7QM8GLY3E1FPCX4h7N4RtnuoPpvEpsl
/K4XQ1p/8Uehe6Izg0BpvQ7A256/+UW3lkwlonR7UaOX/+gkEdxuxlC/
41nX5fI9G5QFrV7H8B7ezlVF/uLz4nXyH4mzz496x4iTMEoHfoAdMinL C7A=
example.                    86400 IN     SOA    a.nic.dns.blablabla.
hostmaster.dns.blablabla. 2017072305 86400 14400 2592000 3600
```

C Checklist de Implementação do DNSSEC

C.1 Iniciação e preparação

❑ Definir a implementação do DNSSEC como um projeto

Gerir todo o processo como um projeto com uma data de início, uma data de fim prevista e resultados claros utilizando uma abordagem de gestão de projetos

❑ Documentar o sistema existente

Ter uma documentação atualizada que descreva o sistema e os processos em uso

❑ Auditar a infraestrutura existente

Corrigir quaisquer deficiências no sistema atual antes da implementação do DNSSEC

❑ Envolver as partes interessadas

Preparar a sua compreensão e preparação para a implementação do DNSSEC

❑ Definir e seguir um plano de formação

Dar aos seus colaboradores e às partes interessadas os conhecimentos e competências necessários para a implementação do DNSSEC

C.2 Implementação e monitorização

❑ Redigir um DP ou DPS

Publicar o enquadramento operacional DNSSEC aplicável na zona

❑ Redigir um plano de implementação do DNSSEC

Documentar a estratégia e as etapas da implementação global. Vários itens da lista de verificação podem ser abordados neste documento.

❑ Redigir e validar os processos e procedimentos de operações DNSSEC *Documentar os procedimentos para os seus requisitos e ambiente*

❑ Escolher um cenário de implementação do DNSSEC

Identificar o modelo de implementação do DNSSEC

❑ Identificar e adquirir novos materiais e equipamentos *Adquirir novos equipamentos e materiais*

❑ Selecionar os parâmetros de assinatura DNSSEC

Atribuir valores a um conjunto de parâmetros DNSSEC

❑ Construir um banco de ensaio DNSSEC

Redigir, executar e validar casos de teste para que a assinatura da zona se familiarize com os processos e operações do DNSSEC

❑ Planear o go-live e preparar uma solução de recurso

Preparar e documentar o go-live no ambiente de produção, bem como os procedimentos de monitorização e de recurso

❑ Go-live e monitorizar

Implementar e monitorizar a assinatura DNSSEC no ambiente de produção

❑ Planear a publicação do DS dos registrants

Promover o DNSSEC, preparar para receber e processar registos DS de subdomínios

❑ Publicar o DS dos registrants

Anunciar o DS dos subdomínios na zona ccTLD

❑ Documentar as lições aprendidas

Compilar as lições e experiências aprendidas em cada etapa do processo

D Outras leituras

- *Major DNSSEC Outages and Validation Failures*, IANIX: https://ianix.com/pub/dnssec-outages.html
- *DNSSEC: The long and bumpy road of algorithm deployment*, APNIC, https://blog.apnic.net/2020/12/01/dnssec-the-long-and-bumpy-road-of-algorithm-deployment/
- *DNSSEC Infrastructure Audit Framework*, NLnet Labs, https://nlnetlabs.nl/downloads/publications/dns-audit-framework-1.0.pdf

- *Root DNSSEC information*, IANA, https://www.iana.org/dnssec
- *Frequently Asked Questions about DNSSEC*, SIDN, https://www.sidn.nl/en/faq/dnssec
- RFC 6781, *DNSSEC Operational Practices v2,* https://www.rfc-editor.org/rfc/rfc6781.html

1. RFC 6841, *A Framework for DNSSEC Policies and DNSSEC Practice Statements,* https://www.rfc-editor.org/rfc/rfc6841.html

2. RFC 8078, *Managing DS Records from the Parent via CDS/CDNSKey,* https://www.rfc-editor.org/rfc/rfc8078.html
3. RFC 8624, *Algorithm Implementation Requirements and Usage Guidance for DNSSEC,* https://www.rfc-editor.org/rfc/rfc8624.html