dnssec•pt Tutorial

.pt

índice

O que é o DNSSEC

DNSSEC (Domain Name System Security Extensions) é o nome dado às extensões de segurança ao protocolo DNS (Domain Name System) concebidas para proteger e autenticar o tráfego DNS. Estas extensões fazem uso da tecnologia de criptografia assimétrica para assegurar a autenticidade e a integridade da informação trocada entre servidores DNS e entre estes e as aplicações do utilizador. Os mecanismos de segurança previstos no DNSSEC são complementares e transparentes para o utilizador, não interferindo, desta forma, com o normal funcionamento do protocolo DNS.

A sua importância

Para compreender a importância do DNSSEC é relevante apresentar uma breve referência ao funcionamento do Sistema de Nomes de Domínio, mais conhecido como DNS, uma das ferramentas fundamentais para o funcionamento da Internet que permite localizar e resolver nomes de domínio em endereços IP e vice-versa.

Este sistema garante dois objetivos essenciais:

- A possibilidade que dá ao ser humano de se abstrair de endereços de rede (endereços IP) cuja memorização é complexa, ao mesmo tempo que permite alterações desses endereços IP sem que o utilizador tenha que conhecer essa alteração para continuar a usar um serviço;

- A garantia que as máquinas e os seus nomes sejam geridos de forma hierárquica e distribuída com o Root Server mundial no topo da hierarquia e com a informação distribuída por milhares de servidores de nomes existentes na Internet, pressuposto do seu sucesso enquanto rede global – não sendo necessário contactar uma entidade central sempre que se efetue uma alteração ou uma adição de novos dispositivos na Internet.

A especificação inicial do DNS, desenhado na década de 80, quando a Internet não tinha a dimensão que conhecemos hoje, não incorporava quaisquer políticas ou mecanismos de segurança. Pelo contrário, o seu desenho dá primazia a aspetos de eficácia, eficiência e escalabilidade. Por este facto, a especificação possuí algumas vulnerabilidades de segurança que têm vindo a ser exploradas maliciosamente com o objetivo de induzir erros na resolução de nomes DNS associadas, nomeadamente, à autenticidade dos sites e à integridade dos dados transmitidos.

Com o objetivo de mitigar um conjunto de vulnerabilidades e vetores de ataques conhecidos, a Internet Engineering Taskforce (IETF), organização responsável pelos padrões de protocolo DNS, procurou encontrar uma solução que fortalecesse a autenticação do protocolo DNS, sem comprometer o seu normal funcionamento e a infraestrutura que depende deste, foram então criadas as extensões de segurança ao DNS, designadas DNSSEC (DNS Security Extensions).

Em suma, as extensões de DNSSEC visam melhorar a confiabilidade dos utilizadores nos serviços prestados *online*, através de um sistema de resolução de nomes mais seguro, reduzindo o risco de manipulação de dados e informações, contribuindo, nomeadamente, para:

- Suprimir fragilidades do protocolo DNS;
- Prevenir ataques do tipo *man-in-the middle* e *cache poisoning*;
- Reduzir o risco de manipulação de informação;
- Reforçar a fiabilidade do sistema.

Com o crescimento na adoção de DNSSEC, o DNS pode ainda tornar-se uma base segura para outros protocolos que requerem a salvaguarda de dados, é neste sentido que têm sido desenvolvidos novos protocolos com dependência do DNSSEC, nomeadamente: DANE (DNS-based Authentication of Named Entities), DKIM (DomainKeysIdentifiedMail); DMARC (Domain-based Message Authentication, Reporting & Conformance).

Como Funciona o DNSSEC

O DNSSEC tem por base a utilização de criptografia assimétrica, tecnologia com a qual os dados DNS são assinados, onde são utilizados dois tipos de chaves criptográficas distintas, mas relacionadas entre si:

- **Zone Signing Key (ZSK)** – Par de chaves pública/privada que assina a zona. A chave privada é utilizada para assinar o conjunto de resource records na zona (RRSet) designado por RRSIG. A chave pública é colocada na zona DNS para permitir a validação do RRSIG.

- **Key Signing Key (KSK)** – Par de chaves pública/privada que assina outras chaves. A chave privada é utilizada para assinar a chave ZSK. A chave pública é colocada na zona DNS para validar a chave ZSK assinada.

Quando um domínio se encontra "assinado", um servidor de nomes DNS pode autenticar as respostas que obtém, garantindo a autenticidade da origem e proteção da integridade dos dados DNS, protegendo assim o utilizador de ataques, como por exemplo, de injeção de informação corrupta (*DNS spoofing*).

Em termos técnicos e de segurança as principais responsabilidades em relação à utilização de criptografia assimétrica no DNSSEC são:

- Confinamento rigoroso das chaves privadas aos legítimos detentores;
- Distribuição fidedigna de chaves públicas a todos os que delas necessitem;
- Atualização da informação da assinatura da zona na hierarquia superior;
- Correta manutenção da zona assinada;
- Gestão do tempo de vida dos pares de chaves.

Os pares de chaves assimétricas são personalizados, ou seja, são associados a pessoas, serviços ou servidores. A componente privada deve ser mantida em segredo, devendo ser apenas do conhecimento e da utilização da entidade a que se encontra associada.

A chave pública deve ser ampla e publicamente divulgada para poder ser utilizada por qualquer entidade, sendo também publicada no DNS na forma de resource record designado DNSKEY. Utilizando a chave pública torna-se assim possível verificar e validar uma assinatura que tenha sido gerada por uma chave privada.

Para este processo resultar é necessário que se confie numa chave pública antes de verificar a assinatura. Uma vez que é difícil confiar em todas as chaves existentes na Internet, foi criada uma hierarquia de confiança semelhante à estrutura em hierarquia do DNS que se designa por *chain trust* e desta forma confiando apenas numa única chave pública, neste caso na chave da root ".", é possível verificar todas as assinaturas.

Para se obter uma cadeia de segurança é necessário que um resumo da chave pública, nomeadamente o resource record DS, seja enviado para o nível superior da hierarquia. O nível superior insere na sua zona a informação de assinatura referente à zona filha em forma de resource record DS, garantindo assim a autenticidade da informação após assinar a mesma.

O ciclo repete-se e a informação da chave pública deste nível superior é enviada para o nível superior seguinte acabando esta cadeia hierárquica de assinaturas na root.

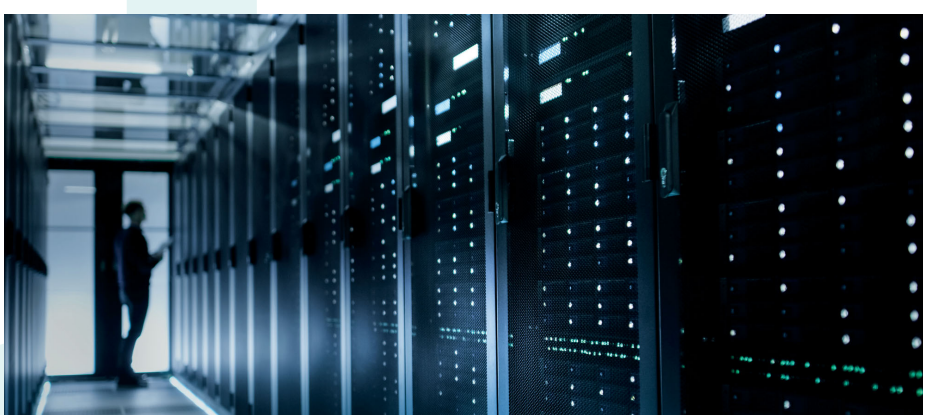
Os registos de DNS que o DNSSEC adiciona de forma a conseguir fazer validação segura são os seguintes:

- **DNSKEY (Public Key)** - Chave pública;
- **RRSIG (Resource Record Signature)** - Assinatura digital do RRset;
- **NSEC (Next Secure)** – Resposta autenticada da não existência de um domínio, fornece ainda indicação do próximo nome seguro e os tipos de RRsets existentes para esse nome;
- **NSEC3 (Next Secure)** – Síntese autenticada da não existência de um domínio ou conjunto de resource records associados a um domínio. Este registo é uma versão atualizada do registo NSEC. O NSEC3 impede a enumeração da zona através do recurso a técnicas de Zone Walking e por isso deve ser utilizado em detrimento do registo NSEC;
- **DS (Delegation Signer)** - Síntese da chave pública que faz a ligação entre um domínio e subdomínio de modo a construir uma cadeia de confiança;

Guidelines para a implementação

Os sistemas operativos mais recentes já se encontram preparados para a utilização de DNSSEC, permitindo assim que a aplicação da tecnologia DNSSEC chegue aos utilizadores finais.

Relativamente aos sistemas a operarem como resolvers é necessário confirmar que estes se encontram preparados para a validação de DNSSEC, sendo que aqui o papel mais importante cabe aos fornecedores de serviços de Internet, ISP (Internet Service Providers) e das empresas que gerem os seus serviços de resolução de nomes, nomeadamente servidores de nomes recursivos.



Para um titular de um domínio, é necessário que o titular solicite ao responsável técnico associado ao domínio que preceda à configuração do seu domínio com DNSSEC.

Para ter um domínio assinado com DNSSEC é necessário configurar o domínio seguindo procedimentos recomendados (DNSSEC Operational Practices, Version 2), sendo que os que são considerados mais relevantes são os seguintes:

- Utilizar ferramentas e software nas versões estáveis mais recentes e proceder regularmente às suas atualizações, aplicando patchs de segurança quando necessário;
- Configurar corretamente os dados DNS na zona e os respetivos servidores de nomes autoritários onde a zona se encontra delegada;
- Gerar uma chave que assina a zona (ZSK - Zone Signing Key);
- Gerar uma chave que assina chaves (KSK - Key Signing Key);
- Assinar todos os conjuntos de resource records (RRSet) existentes na zona com a ZSK;
- Assinar todas as chaves (DNSKEYs) com a KSK;
- Criar o Delegation Signer (DS) através da KSK;

  Solicitar submissão do resource record DS no TLD da zona hierarquicamente superior;

- Assinar a zona sempre que existe alteração aos dados DNS (resource records);
- Desenvolver automatismos de assinatura de domínios, para que todas as zonas com DNSSEC sejam assinadas automaticamente, mesmo quando não existem alterações, permitindo desta forma prolongar a validade das assinaturas digitais geradas, sem que estas nunca cheguem a expirar.
- Recomenda-se o planeamento de rotação de chaves em caso de emergência ou programado.

O .PT disponibiliza apoio técnico na configuração destas extensões de segurança em domínios sob o .pt, mais informações disponíveis em: https://www.dns.pt/pt/seguranca/dnssec/.

Links oficiais de referência

ENISA: Good practices guide for deploying DNSSEC

https://www.enisa.europa.eu/publications/gpgdnssec/at_download/fullReport

IANA: Domain Name System Security (DNSSEC) Algorithm Numbers

https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml

ICANN: DNSSEC – What Is It and Why Is It Important?

https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en

IETF: DNSSEC Operational Practices

https://tools.ietf.org/pdf/rfc6781.pdf

ISC: BIND DNSSEC Guide

https://ftp.isc.org/isc/dnssec-guide/dnssec-guide.pdf

10 razões para assinar um domínio com DNSSEC

- Os principais servidores recursivos abertos efetuam resolução DNSSEC;
- Já existem diversos fornecedores de serviço DNS com opção de ativação de DNSSEC;
- Existem ISPs que fazem validação DNSSEC;
- Disponíveis ferramentas para desenvolvimento de DNSSEC;
- Gera segurança e segurança nos seus clientes;
- Protege o utilizador final;
- Preferência, na comunidade, para a adoção de infraestruturas num modelo seguro;
- Boa prática de segurança, sendo a segurança um fator de diferenciação;
- A adoção de DNSSEC permite a implementação de novos protocolos;
- DNSSEC é a evolução natural DNS contribuindo para uma Internet mais segura;

Produção: junho 2019 ■ Grafismo: dns.pt