O que é o DNSSEC?

DNSSEC 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.

Porque é o DNSSEC necessário?

Com a, cada vez maior, dependência do cidadão comum nas tecnologias da comunicação e da informação e da Internet em particular, tem vindo a crescer a preocupação dos utilizadores e o grau de importância das questões relacionadas com a segurança das transacções electrónicas. Esta preocupação resulta da exposição mediática de ataques feitos a serviços em linha, explorando vulnerabilidades nas aplicações e nos serviços básicos da Internet.

Como consequência diversos países identificaram a segurança informática e a confiança dos utilizadores nos serviços prestados em linha como o principal constrangimento ao crescimento do comércio electrónico. Noutro contexto, as autoridades responsáveis pela protecção de infra-estruturas críticas da informação têm vindo a implementar medidas extraordinárias para reforçar a segurança do ciberespaço, na qual o DNS assume um papel de destaque.

Para responder a estas necessidades for criado, pelas entidades normalizadoras, o DNSSEC, um conjunto de extensões realizadas ao protocolo DNS (*Domain Name System*) que vem mitigar uma série de vulnerabilidades e de vectores de ataque bem conhecidos a serviços em linha, melhorando a qualidade e a confiança dos utilizadores nestes.

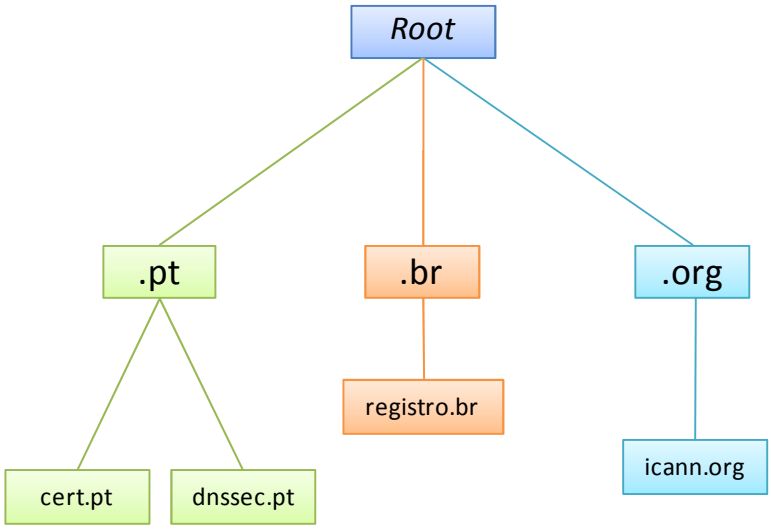
As extensões DNSSEC visam melhorar a confiabilidade dos utilizadores nos serviços prestados em linha. O DNSSEC vem nomeadamente:

- 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.

⇨ Como é que o DNS funciona?

O sistema de nomes de domínio, mais conhecido por DNS é uma das ferramentas fundamentais para o funcionamento da Internet que permite localizar e resolver nomes de domínio em endereços IP e vice-versa.

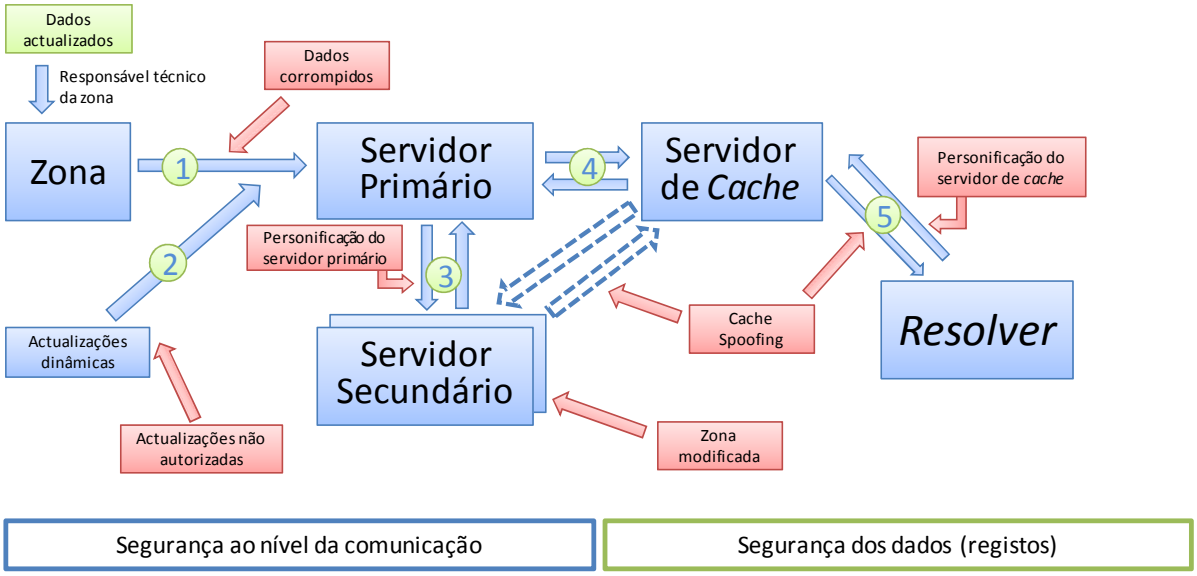
Para além de permitir ao ser humano abstrair-se do conceito de endereços de rede (endereços IP sejam eles em IPv4 ou IPv6) cuja memorização é complexa, ao mesmo tempo que permite alterações desses endereços IP sem que o utilizador tenha que conhecer essa alteração para continuar a usar um serviço, simplificando todo o processo, também garante que as máquinas e os seus nomes são geridos de forma hierárquica e distribuída com um servidor "Root" 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 e não sendo necessário contactar uma entidade central sempre que se efectue uma alteração ou uma adição de informação DNS na Internet.



O DNS, baseado no conceito de descentralização, tem três grandes componentes: a base de dados; o servidor; e o cliente. A base de dados é distribuída e contém os *resource records (RRs)* dos domínios que definem as zonas de domínios numa árvore DNS. Estes RRs são registos que delegam a autoridade de configuração de uma zona a uma determinada entidade.

O DNS faculta a resolução de nomes em ambas as direcções, isto é, dado um domínio, devolve o endereço IP apropriado e vice versa, através da utilização dos *resource records*. Estes *RRs* fazem parte da configuração dos domínios e encontram-se armazenados em ficheiros de zona que contém os dados necessários para resolver os pedidos de nomes associados ao domínio da qual a zona é responsável.

A especificação inicial do DNS não contempla quaisquer políticas ou mecanismos de segurança para evitar ataques à resolução de nomes. Pelo contrário, o seu desenho consiste fundamentalmente e dá primazia a aspectos de eficácia, eficiência e escalabilidade. Por este facto, a especificação possuí diversas vulnerabilidades de segurança que têm vindo a ser exploradas aos longo dos anos por forma a induzir erros na resolução de nomes DNS.

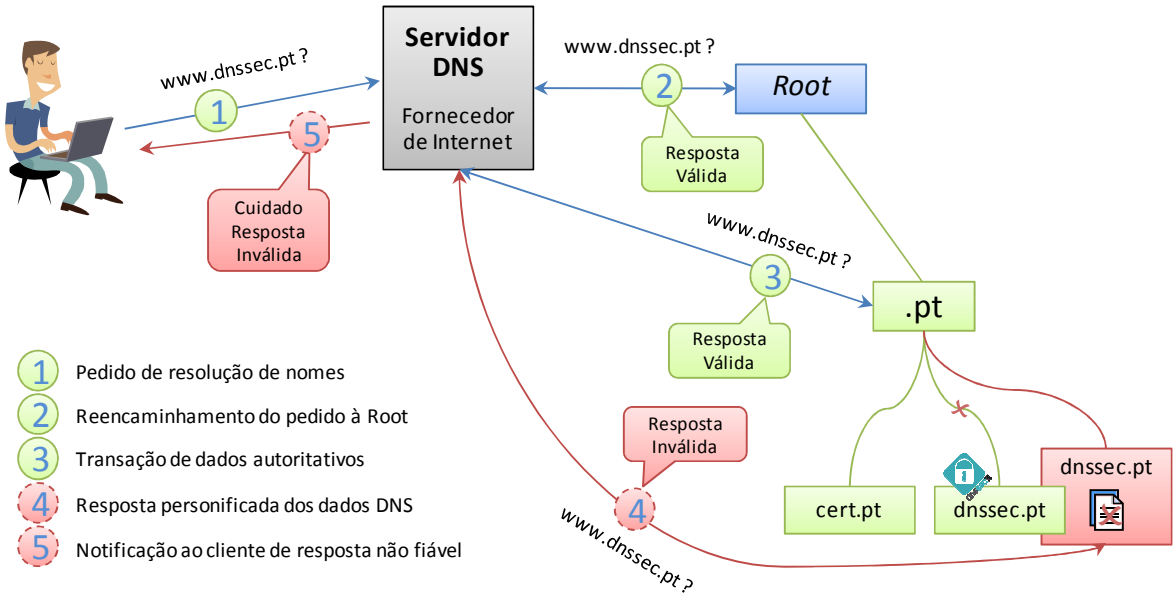


Sendo o DNS originariamente desenhado sem as necessárias preocupações de segurança, mas perante a crescente importância da informação que este serviço fornece, tornou-se imprescindível no percurso de expansão da Internet assegurar a correcta comunicação entre os sistemas informáticos e surgem diversas políticas e mecanismos que procuram eliminar e minimizar os riscos, como é o caso das extensões de segurança DNSSEC.

⇨ Como funciona o DNSSEC?

O DNSSEC tem por base a utilização de criptografia assimétrica, tecnologia com a qual os dados DNS são assinados.

Quando um domínio se encontra "assinado", um servidor de nomes DNS pode autenticar as respostas que obtém protegendo assim o utilizador de ataques, como por exemplo, de injecção de informação corrupta na memória temporária do servidor.



A criptografia assimétrica utiliza um par de chaves distintas mas relacionadas entre si, são estas: a chave pública e a chave privada.

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

- Delimitação rigorosa das chaves privadas aos legítimos detentores;
- Distribuição fidedigna de chaves públicas a todos os que delas necessitem;
- Actualização da informação da assinatura da zona com a hierarquia superior;
- Correcta manutenção da zona assinada;
- Gestão do tempo de vida dos pares de chaves.

Em contraponto com a implementação tradicional de DNS, com uma solução DNSSEC e tal como observado na figura consegue-se detectar uma alteração de informação DNS (ponto 4 da figura acima apresentada), e proceder à necessária notificação ao utilizador (ponto 5 da figura) levando a que essa informação seja descartada.

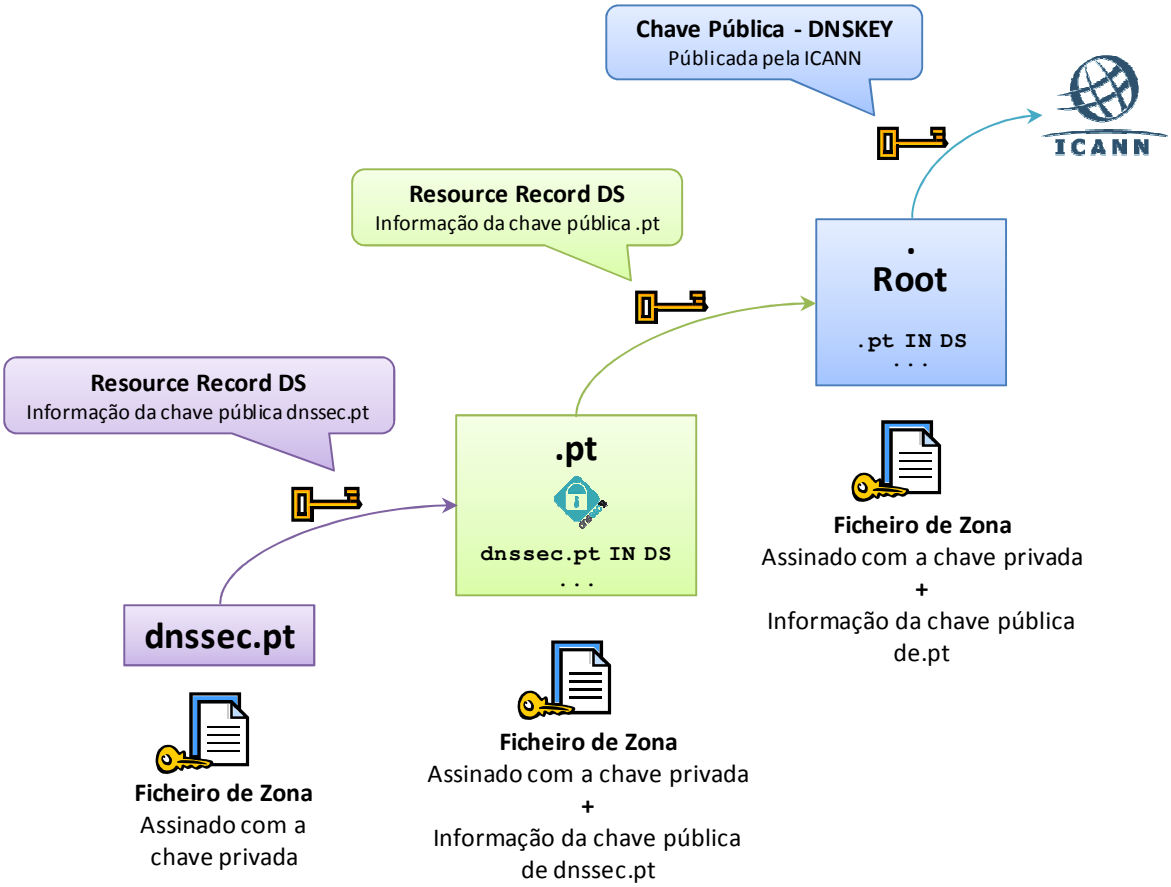
⇨ Como são validadas as assinaturas DNSSEC?

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 pode, e 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 é possível verificar todas as assinaturas.

⇨ Como se obtém uma cadeia de confiança DNSSEC?



Um resumo da chave pública é 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*.

⇨ O que necessito para poder utilizar DNSSEC?

Ao nível dos utilizadores finais os sistemas operativos mais recentes já se encontram preparados para a utilização de DNSSEC.

Ao nível dos sistemas a operarem como *resolvers* será necessário confirmar que estes estão preparados para a implementação de DNSSEC.

Se é titular de um domínio em .pt, deverá exigir ao seu responsável técnico a configuração do seu domínio com DNSSEC.

O DNS.PT consciente da importância desta matéria dará todo o apoio aos responsáveis técnicos para a configuração destas extensões.

Para essa tarefa disponibilizamos documentação e outra informação relevante em www.dnssec.pt, existe ainda a possibilidade de registar gratuitamente domínios sob a hierarquia dnssec.pt para testes de configuração DNSSEC.

⇨ Estado da Arte?

Para além da implementação portuguesa do DNSSEC que se encontra em fase de conclusão outros países já adoptaram esta tecnologia entre os quais destacamos: Suécia (.se), Porto Rico (.pr), Brasil (.br), Bulgária (.bg) e República Checa (.cz), . Existem também alguns domínios de topo tais como: .gov, .org e .museum.

Brevemente, prevê-se que a *Root* seja também assinada. Com este procedimento será possível propagar a cadeia de confiança a toda a estrutura hierárquica do DNS, simplificando todo o processo.