



Anúncio | Estágio

Atualização Automática dos registos DS (Delegation Signer) em domínios .pt

Orientação: A designar

Enquadramento:

A Associação DNS.PT, doravante designada .PT, é a entidade responsável pela gestão, registo e manutenção de domínios sob .pt, domínio de topo nacional. Trata-se de uma associação privada sem fins lucrativos, que tem como fundadores a FCT, IP - Fundação para a Ciência e a Tecnologia, a Associação da Economia Digital (ACEPI) e a Associação Portuguesa para a Defesa do Consumidor (DECO).

O .PT é uma infraestrutura crítica nacional, tendo desde 2015 a certificação ISO/IEC 27001:2013 e desde 2016 orientado as suas funções também ao referencial da continuidade de negócio ISO 22301:2012.

Um dos objetivos primordiais do .PT é assegurar a segurança e a integridade do sistema de nomes de domínio em Portugal. Alinhado a este valor essencial, integrando as melhores práticas e recomendações nacionais e internacionais a nível técnico, administrativo e estratégico que lhe sejam aplicáveis.

Neste contexto, DNSSEC (Domain Name System Security Extensions), o nome dado às extensões de segurança ao protocolo DNS (Domain Name System) concebidas para proteger e autenticar o tráfego DNS, reveste particular relevância para assegurar a autenticidade e a integridade da informação trocada entre servidores DNS e entre estes e as aplicações do utilizador.

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.

Objetivos:

Este trabalho centra-se na implementação de uma solução automatizada e massiva de DNSSEC, que é uma área crucial para a organização e para a segurança da Internet, e divide-se em dois pontos fundamentais:

- Estudo detalhado sobre os modelos de adoção massiva e automatizada de DNSSEC e o sistema de resolução DNS em .PT, nomeadamente “CDS/CDNSKEY” e “DNSSEC Bootstrapping”. Este estudo descreve o estado da arte da implementação de DNSSEC nos congéneres europeus de referência, incluindo elementos que permitam adequar os parâmetros da solução DNSSEC em .PT, assegurando assim os mais altos níveis de segurança e a fácil adoção desta solução pelos agentes de registo/ISPs.
- Propor um ou mais cenários para uma Infraestrutura de processamento automatizado e massivo de DNSSEC para .PT, responsável pelos processos criptográficos, assente na criticidade do serviço e nas melhores práticas internacionais.

Qual é o problema a resolver?

O processo de validação DNSSEC percorre toda a hierarquia DNS, desde o topo até ao domínio. Para isso utiliza 2 chaves criptográficas (ZSK e KSK), e o resumo criptográfico (digest/hash) num registo DNS do tipo Delegation Signer (DS).

É fundamental manter uma correspondência entre as chaves KSK e os respetivos registos DS na delegação do domínio na zona hierarquicamente acima (pai).

Neste contexto, deve existir um mecanismo que garanta de forma automática e constante esta correspondência, nomeadamente quando ocorrem alterações na chave KSK.

O desafio proposto é elaborar um estudo dos vários mecanismos de atualização automática dos registos DS, e promover a sua implementação tendo em conta os requisitos e características do sistema de gestão de registo de domínios .pt, os agentes de registo, a infraestrutura DNS e a sua segurança inerente.

Plano de Trabalhos:

- Estudar o mecanismo de atualização DS atual;
- Estudar os vários mecanismos/soluções existentes;
- Avaliar a solução que melhor se enquadra ao contexto do .PT;
- Aplicar a solução ao contexto do .PT e produzir a respetiva documentação;
- Avaliar os Gaps relativamente a solução e sugerir melhorias.

Como serão avaliados os resultados?

Espera-se obter um estudo detalhado sobre implementação de automatismos em DNSSEC e propostas/cenários exequíveis de uma Infraestrutura de processamento para .PT, que logrem servir de base ao projeto de implementação pela organização, segundo os requisitos definidos.

Condições a propor ao candidato:

- Estágio de 6 meses, com início em setembro.
- Negociável, duração diária de 7 horas e semanal de 14 horas em regime híbrido na sede do .PT.
- Subsídio de estágio proporcional.
- Subsídio de alimentação correspondente aos dias trabalhados.

Localização: Associação DNS.PT/ Universidade (formato híbrido).

Observações: Tese escrita em português.