



JORNADAS
RCTS
REDE CIÊNCIA, TECNOLOGIA E SOCIEDADE

LISBOA - 9,10,11
DE FEVEREIRO 2010
Grande Auditório
do LNEC - Lisboa

Deployment DNSSEC

Estado da arte na RCTS

Sara Monteiro

10 de Fevereiro de 2010



Fundação para a Computação Científica Nacional
Foundation for National Scientific Computing





- Âmbito
 - Objectivos
 - Vulnerabilidades do DNS
 - O que é o DNSSEC?
 - Desenvolvimentos no .pt
 - Desafio à RCTS
 - Estado da arte
 - Plano de trabalhos
-
-



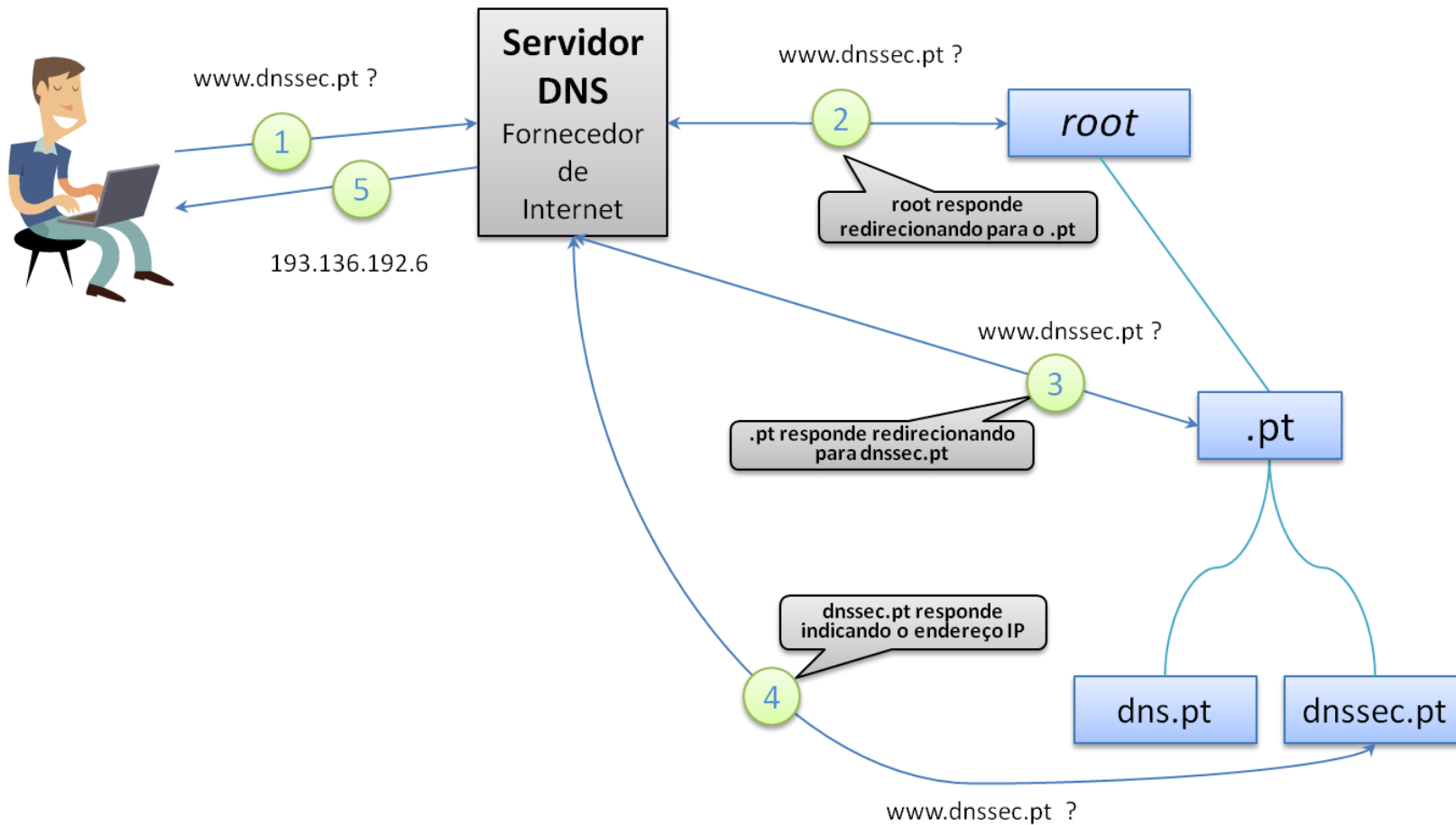
- Estado de desenvolvimento do DNSSEC na RCTS e discussão de abordagens, constrangimentos e plano de trabalhos
-
-



- Fornecer um serviço DNS mais seguro
 - Promover a implementação de DNSSEC
 - Facilitar a adopção de DNSSEC
 - Fornecer documentação teórica e prática de desenvolvimento
 - Partilhar conhecimento e experiência
 - Aplicar as melhores práticas no que concerne à segurança e protecção dos dados
-

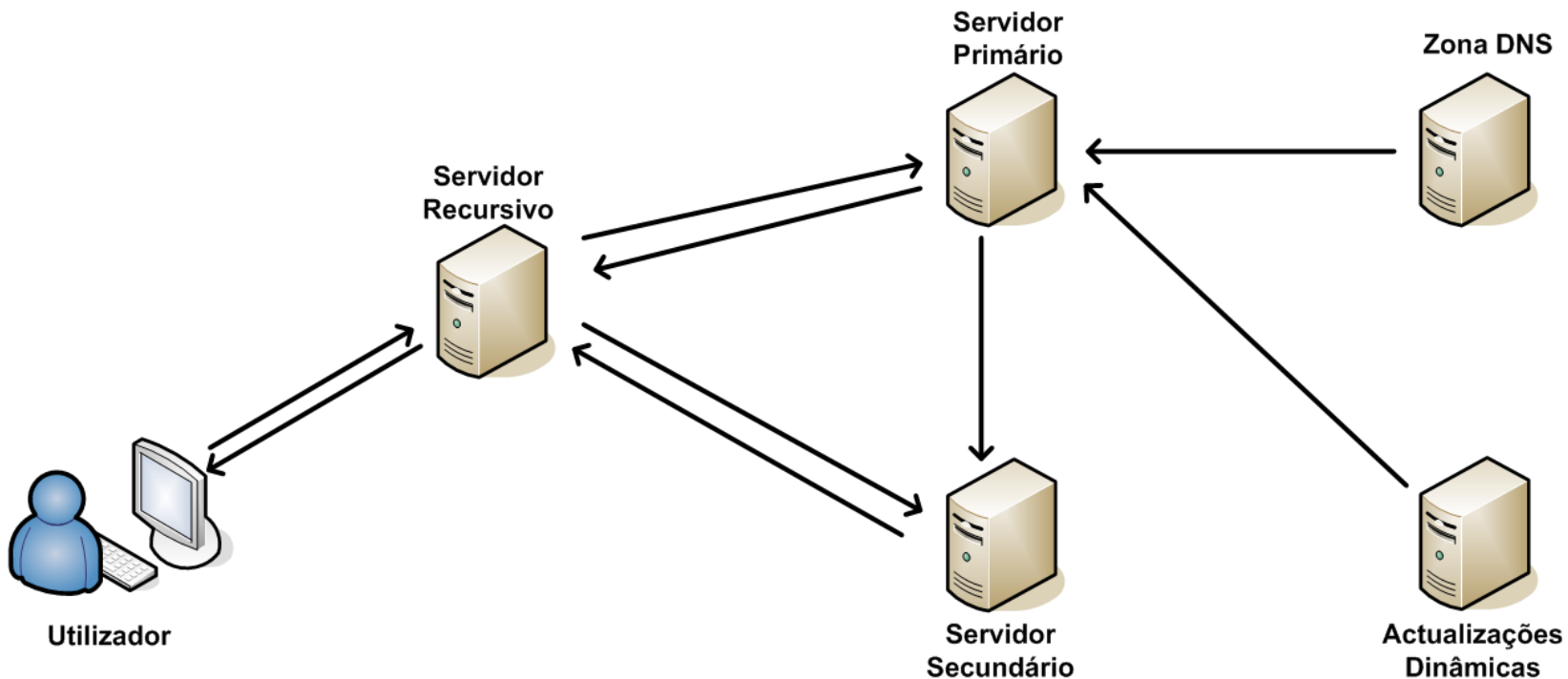


Vulnerabilidades do DNS



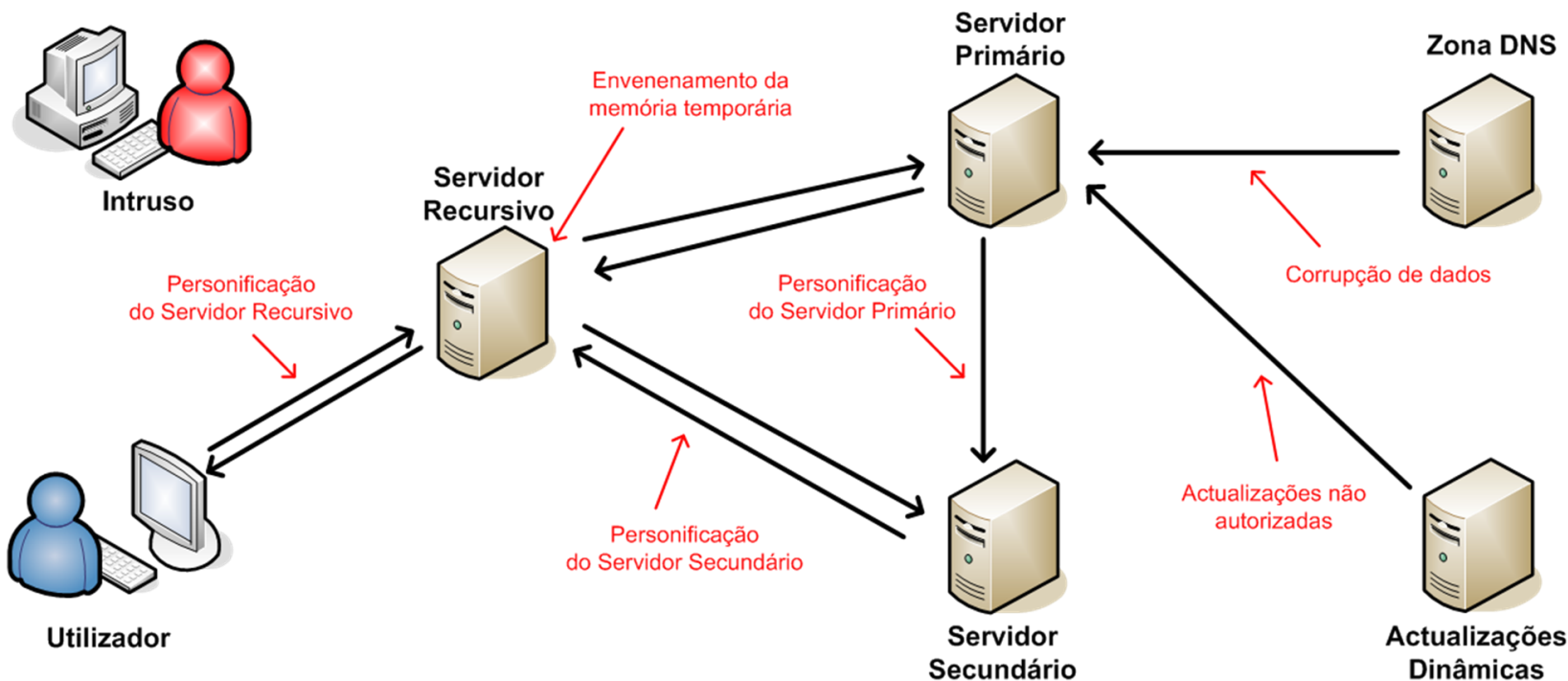


Vulnerabilidades do DNS



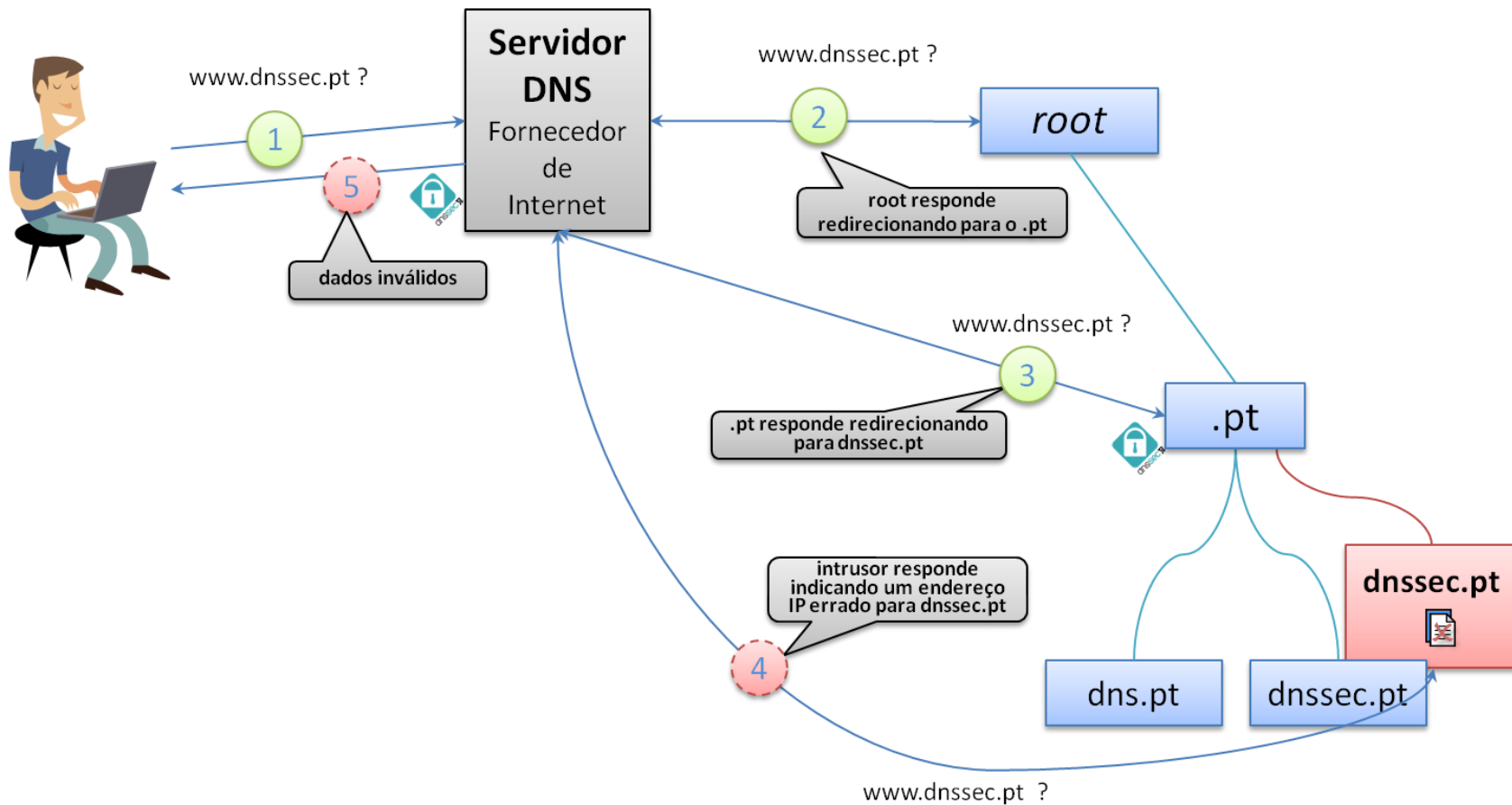


Vulnerabilidades do DNS





O que é o DNSSEC?





Domain Names System Security Extensions:

- Extensão de segurança ao protocolo DNS
 - Garante integridade dos dados
 - Permite autenticação da origem
 - Verifica a inexistência de um domínio
 - Evita manipulação da memória de cache
 - Protege de transmissões modificadas
 - Criptografia assimétrica
 - Assinaturas Digitais
-



- Introduz novos tipos de *Resource Records*:
 - DNSKEY (*Public Key*), RRSIG (*Resource Record Digital Signature*), NSEC/NSEC3 (*Next Secure*), and DS (*Delegation Signer*)
 - DNSKEY – Chave pública
 - RRSIG – Assinatura digital de um conjunto de *RRs*
 - NSEC/NSEC3 – Resposta autenticada (em forma de síntese no caso de NSEC3) da não existência de um domínio, fornecendo também a indicação do próximo nome seguro e os tipos de *RRsets* existentes para esse domínio
 - DS – Síntese da chave pública que faz a ligação entre um domínio e subdomínio de modo a construir uma cadeia de confiança
-

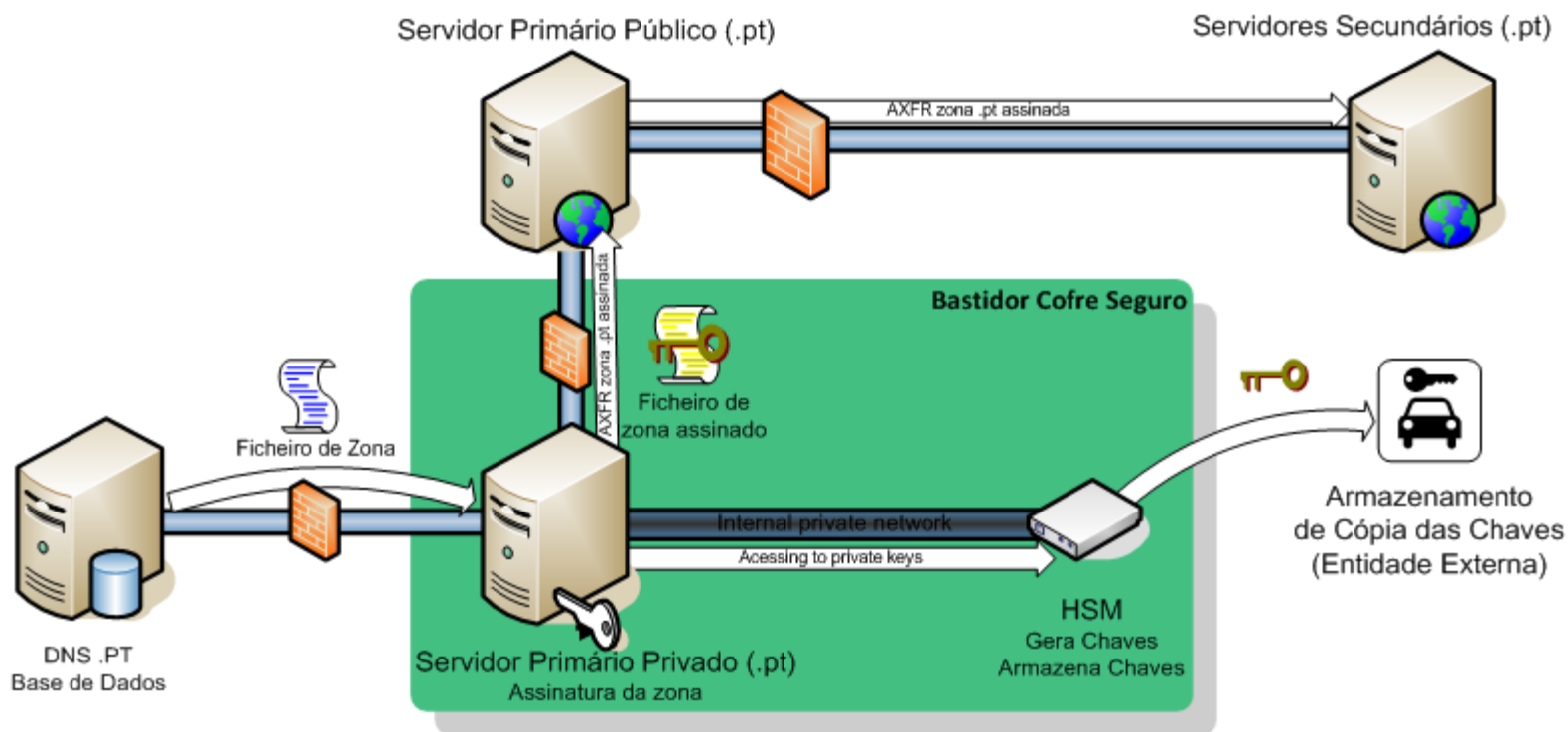


- Organização de conferências, sessões e workshops
 - Publicação de comunicados de imprensa, folhetos e notícias online
 - Divulgação de mailing-lists para pedidos e questões para dev@dnssec.pt e info@dnssec.pt respectivamente
 - Informação e documentação disponível em <http://www.dnssec.pt>
 - Disponibilização de contacto directo por telefone para apoio técnico de DNSSEC
-



Desenvolvimentos no .pt

- Adquirida infra-estrutura de alto nível de segurança, estabilidade e desempenho:





- Disponibilizado interface gráfico no sistema online para gestão técnica do DNSSEC:

Gestão de Domínios	Pesquisa Domínio	Registrars	Whois
--------------------	------------------	------------	-------

Gestão de Domínios Online

Processo	Domínio	Hierarquia	Estado	Data Submissão	Facturado até	ET	EG	RA	RT
396741	saramonteiro	.nome.pt	ACTIVE	03/12/2009		S	N	N	S

Consulta: [Ficha de Processo](#)

Opções ET: [Remover Domínio](#) | [Senha p/ alteração EG](#) | [Assumir a Gestão](#) |

Opções RT: [Alterações técnicas](#) | [Pedido de Avaliação](#) | [DNSSEC](#) |

DNSSEC

A tabela que se segue contém informação relativa às chaves associadas ao seu domínio no âmbito da assinatura de domínios por DNSSEC.

Para publicar novas chaves, remover chaves anteriormente publicadas ou modificar o estado de chaves referentes à sua zona deverá efectuar aqui as respectivas alterações:

Key Tag	Algoritmo	Tipo	Resumo	Activa	Desde	
28824	7: RSA/SHA-1 (NSEC3)	1	4C15DE1F351C204E31B8D1CE2972E147D05A29C1	Sim	27/01/2010 16:14	<input type="checkbox"/>

Alterações:

[Activar](#)

[Desactivar](#)

[Eliminar](#)



- Zona .pt encontra-se assinada e em produção desde o dia 4 de Janeiro de 2010

```
; <<>> DiG 9.7.0 <<>> @ns.dns.pt pt. ANY +dnssec +multiline
```

```
;; ANSWER SECTION:
```

```
pt.                28800 IN SOA ns.dns.pt. hostmaster.dns.pt. (
                    2010021002 ; serial
                    21600      ; refresh (6 hours)
                    7200       ; retry (2 hours)
                    2592000    ; expire (4 weeks 2 days)
                    300        ; minimum (5 minutes)
                    )
pt.                0 IN RRSIG NSEC3PARAM 7 1 0 20100312094954 (
                    20100210094954 43275 pt.
                    BhdE5rib4RgHqIh2gk2REjQ71qLXla2rImBBfEuR2fIT
                    qWPYvFZXcqVmROv6+C3peHv4uuR/MgHnh2HF9u7O5DQ
                    3N8lrZ2jSWDQZf79LcWgtZZqYRAa9bSPZY99Jbv4Eh6T
                    tzSlVnwhCcILK9FV1IzWqED+rPnFikBpa4MY3ps= )
pt.                0 IN NSEC3PARAM 1 0 10 FCCE
pt.                28800 IN RRSIG DNSKEY 7 1 28800 20100312094954 (
                    20100210094954 18303 pt.
```



- Lançado em Novembro de 2009
 - Inserido no esforço de promoção do DNSSEC junto da comunidade Internet portuguesa
 - O sector académico desempenha um papel de destaque na adopção das novas tecnologias
 - Foi proposta a adopção de DNSSEC dentro da RCTS
-
-



- Domínios da RCTS que se encontram assinados com DNSSEC e nos notificaram:
 - ipb.pt (Instituto Politécnico de Bragança)
 - uma.pt (Universidade da Madeira)
 - ipca.pt (Instituto Politécnico do Cávado e do Ave)
 - uatlantica.pt (Universidade Atlântica)
 - Que iniciaram processo de assinatura mas não concluíram:
 - ipg.pt (Instituto Politécnico da Guarda)
-
-



- Principais problemas detectados:
 - Desconhecimento da infra-estrutura global para a resolução de nomes tais como firewalls, switches, servidores, rede...
 - Capacidade de gestão e configuração de diversos tipos de máquinas
 - Configuração de servidores de nomes com diferentes sistemas operativos
 - Ferramentas utilizadas sem compatibilidade para a adopção de DNSSEC
 - Instalação e actualização de software compatível
 - Conhecimentos necessários de DNS e DNSSEC
-
-



- Problemas concretos:
 - Domínios com assinaturas expiradas, quando é realizada uma pesquisa com validação DNSSEC a resposta DNS é recusada dando a ideia de que o domínio não existe ou a máquina se encontra inacessível:

```
; <<>> DiG 9.3.0 <<>> @149.20.64.21 uatlantica.pt ANY +dnssec +multiline

;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 38894
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;uatlantica.pt.          IN ANY
```



- Tamanho dos pacotes DNS incorrectamente limitado a 512 bytes em servidores e firewalls

```
$ dig +short rs.dns-oarc.net txt (Teste)
```

```
rst.x486.rs.dns-oarc.net.
```

```
rst.x454.x486.rs.dns-oarc.net.
```

```
rst.x384.x454.x486.rs.dns-oarc.net.
```

```
"X.X.X.X DNS reply size limit is at least 486 bytes"
```

```
"X.X.X.X lacks EDNS, defaults to 512"
```

- Significa que a máquina X.X.X.X não permite mais que 512 bytes e não tem EDNS configurado
-
-



- Integrar DNSSEC com o sistema EPP
 - Automatizar a alteração de informação por meio de actualizações dinâmicas
 - Enriquecer o conhecimento interno da equipa do .pt relativamente a DNSSEC
 - Organizar workshops de DNSSEC
 - Participar em conferências e “passar a palavra” acerca da adopção de DNSSEC
 - Melhorar o nosso sistema no que diz respeito DNSSEC
-



Obrigada pela vossa atenção



<http://www.dnssec.pt>

dev@dnssec.pt | info@dnssec.pt
