



Fundação para a Computação Científica Nacional
Foundation for National Scientific Computing

DNSSEC no .PT

Acção de Sensibilização DNSSEC

25 de Novembro de 2009



Sara Monteiro

Serviço de Infra-estrutura Técnica DNS.PT

- Âmbito
- Objectivos
- O que é o DNS?
- O que é o DNSSEC?
- Vantagens/Benefícios
- Adopção
- Ferramentas
- Desenvolvimentos
- Trabalho Futuro

Preparar a comunidade de Internet Portuguesa para a adopção de DNSSEC

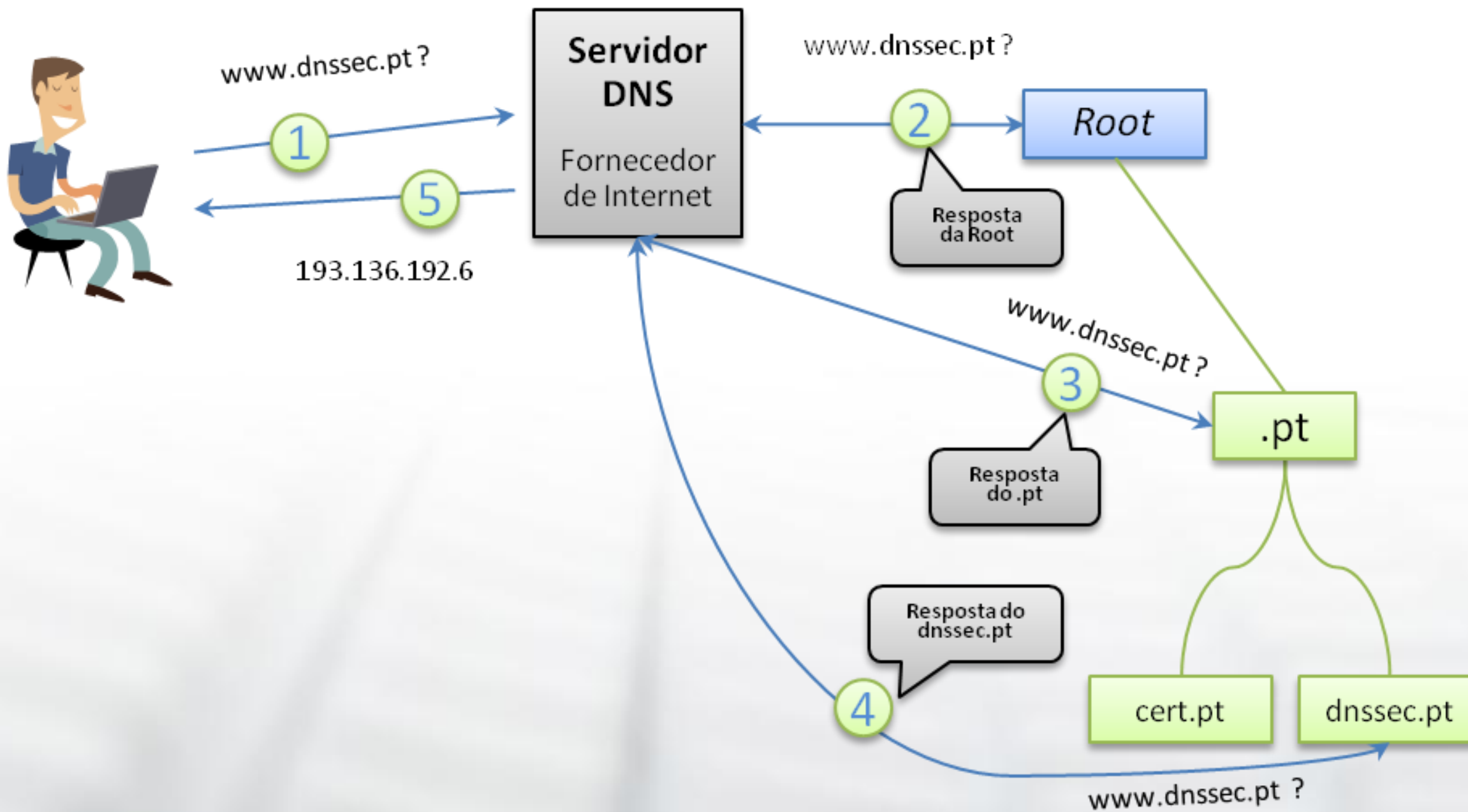


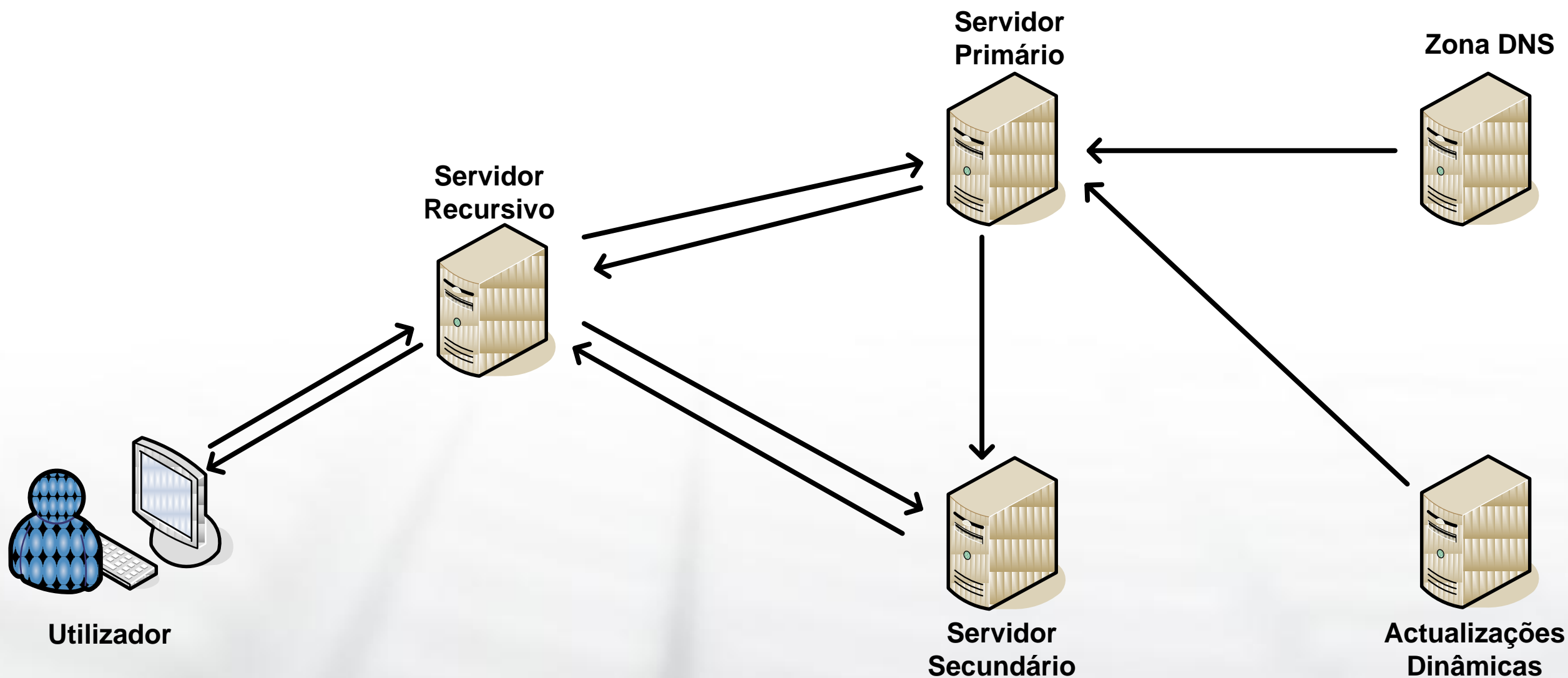
- Promover a implementação de DNSSEC
- Facilitar a adopção de DNSSEC
- Fornecer documentação de desenvolvimento
- Partilhar conhecimento, experiência e aprender da experiência de outros TLDs
- Aplicar as melhores práticas no que diz respeito a segurança e protecção dos dados

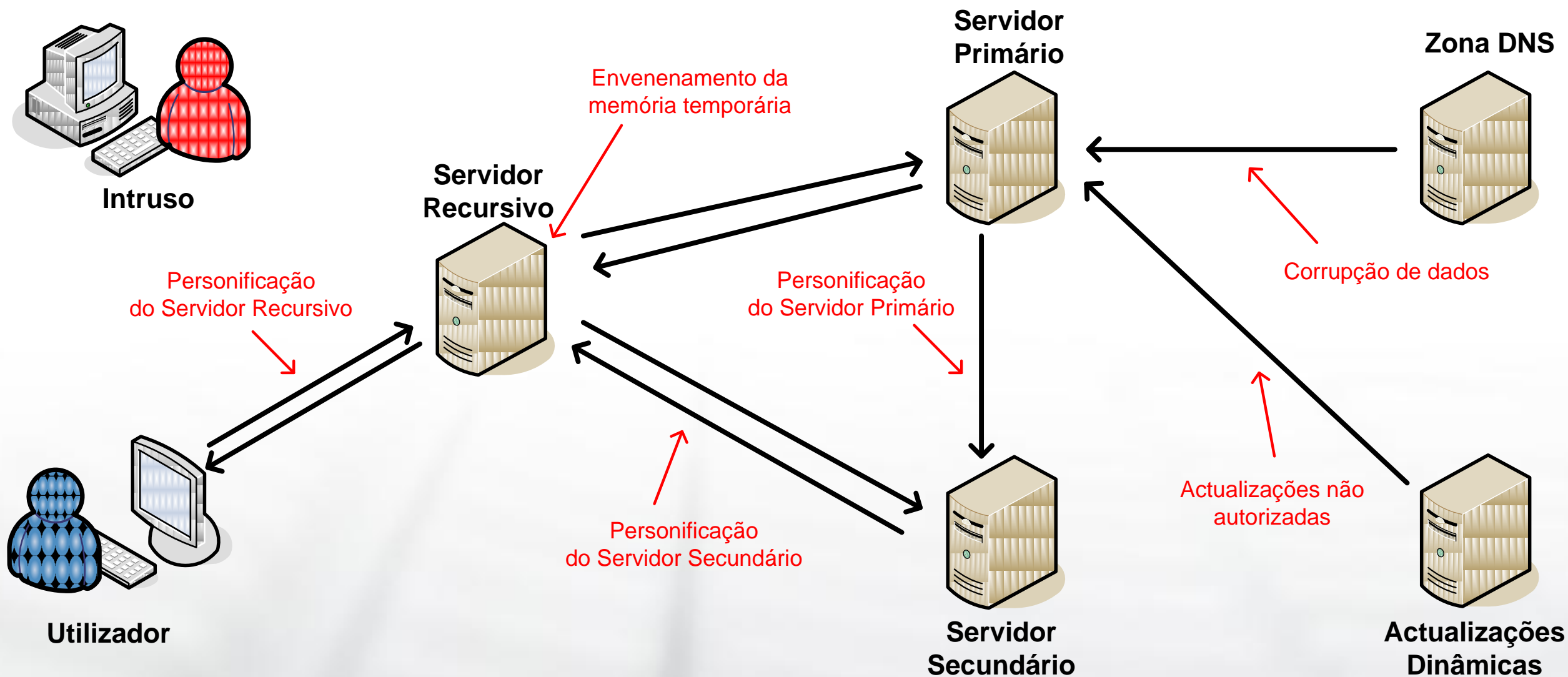
Domain Names System:

- Protocolo de comunicação
- Resolução de nomes em endereços e vice-versa
- Base de dados global e distribuída
- Fundamental para a Internet
- Serviço simples e útil









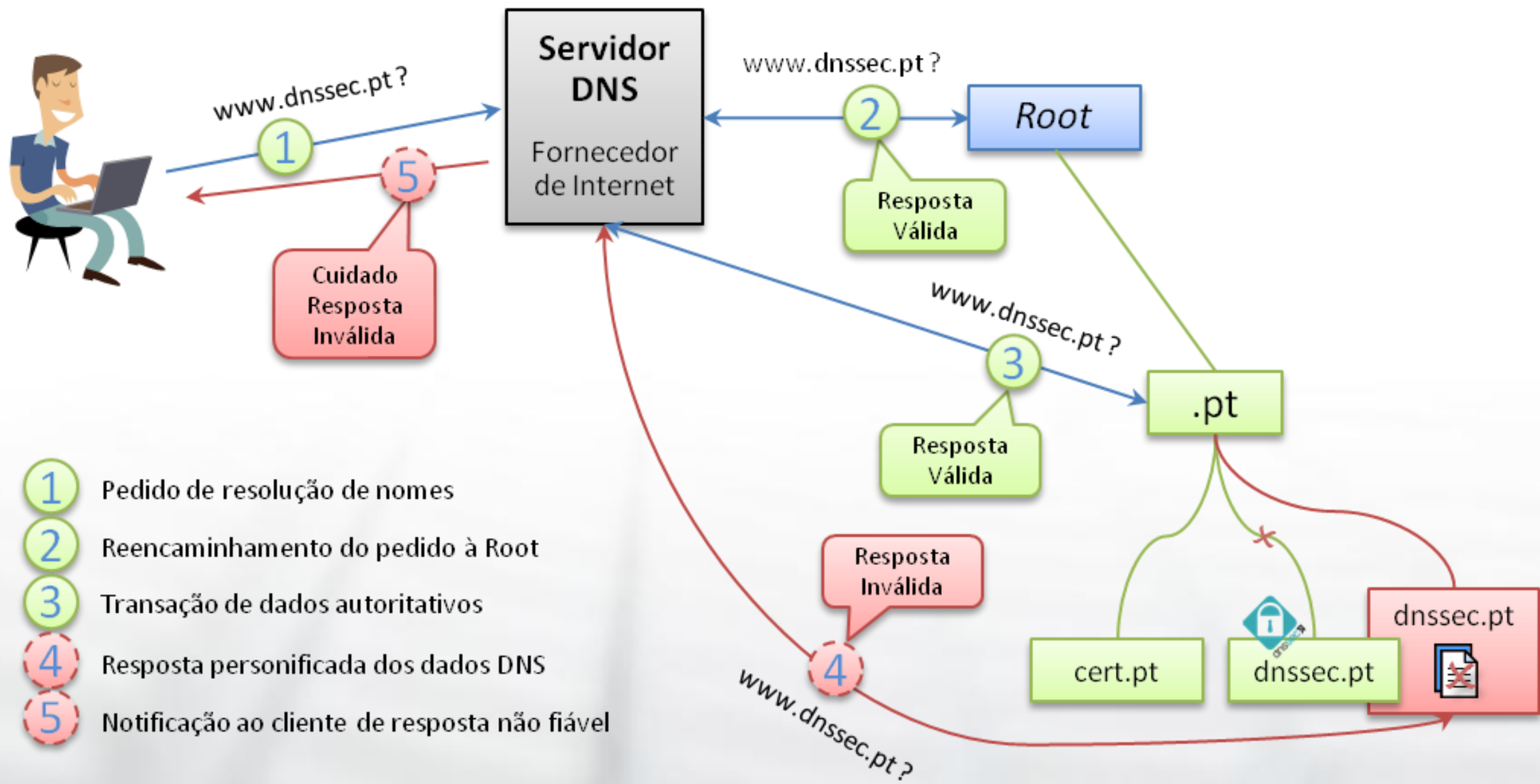
Domain Names System Security Extensions:

- Extensão ao protocolo DNS
 - Compatível com a versão base
- Assinaturas Digitais
 - Os dados DNS são assinados criptograficamente
- Criptografia assimétrica
 - Pares de chaves pública e privada
 - ZSK (*Zone Signing Key*): Chave que assina a zona
 - KSK (*Key Signing Key*): Chave que assina chaves



- Reduz o risco de manipulação indevida de informação DNS garantindo:
 - Autenticação da origem da informação DNS
 - Integridade dos dados DNS
 - Inexistência de um determinado nome domínio
- Introduz novos tipos de dados DNS - *Resource Records*
 - DNSKEY (*Public Key*)
 - RRSIG (*Resource Record Digital Signature*)
 - NSEC/NSEC3 (*Next Secure*)
 - DS (*Delegation Signer*)

- **DNSKEY** - Chave pública
- **RRSIG** - Assinatura Digital de um conjunto de *Resource Records* específico
- **NSEC** - Resposta autenticada da não existência de um domínio, fornecendo também a indicação do próximo nome seguro e os tipos de *RRsets* existentes para esse nome
- **NSEC3** - Síntese autenticada da não existência de um domínio ou conjunto de *Resource Records* associado a um domínio
- **DS** - Síntese da chave pública que faz a ligação entre um domínio e subdomínio de modo a construir uma cadeia de confiança



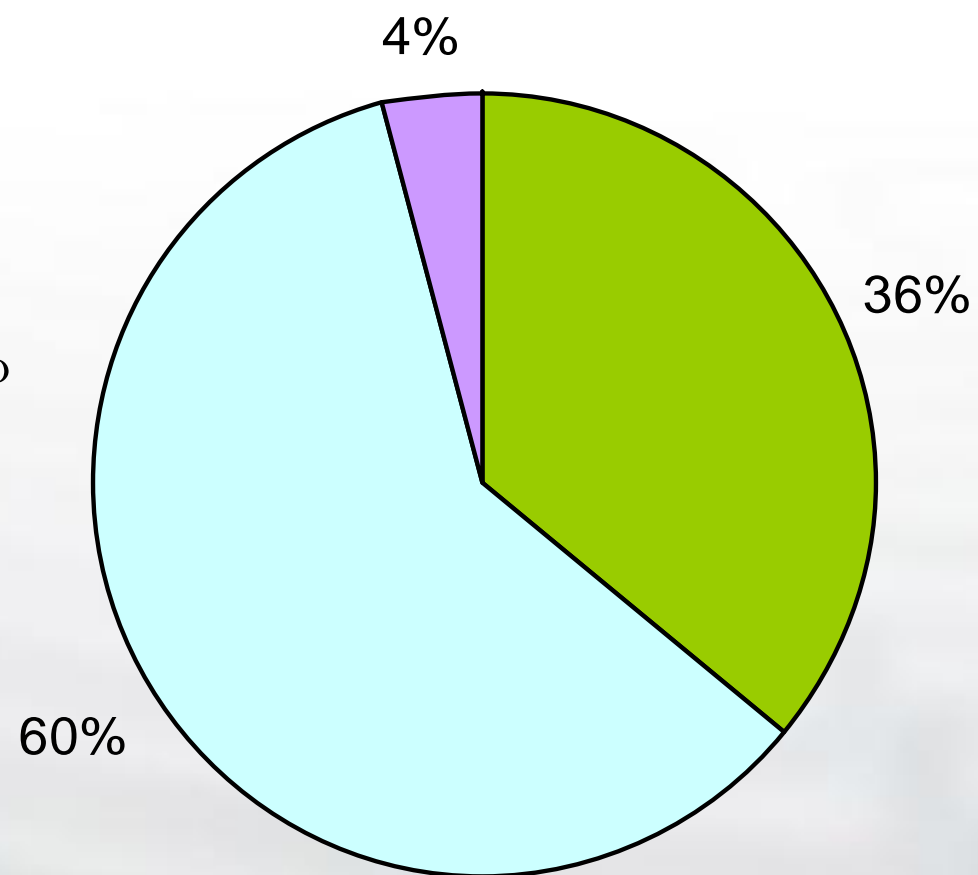
- 1 Pedido de resolução de nomes
- 2 Reencaminhamento do pedido à Root
- 3 Transação de dados autoritativos
- 4 Resposta personalizada dos dados DNS
- 5 Notificação ao cliente de resposta não fiável

- Fornece autenticação da origem da informação
- Garante a integridade dos dados DNS
- Confirma a inexistência de um domínio
- Evita manipulação da memória de cache
 - Pharming, Phishing...
- Protege de transmissões modificadas
 - Man-in-the-Middle, Spoofing...
- Independente dos algoritmos criptográficos
- Fornece confiança no serviço

*Considera a implementação de DNSSEC no ccTLD
.PT uma mais valia para o serviço DNS?*

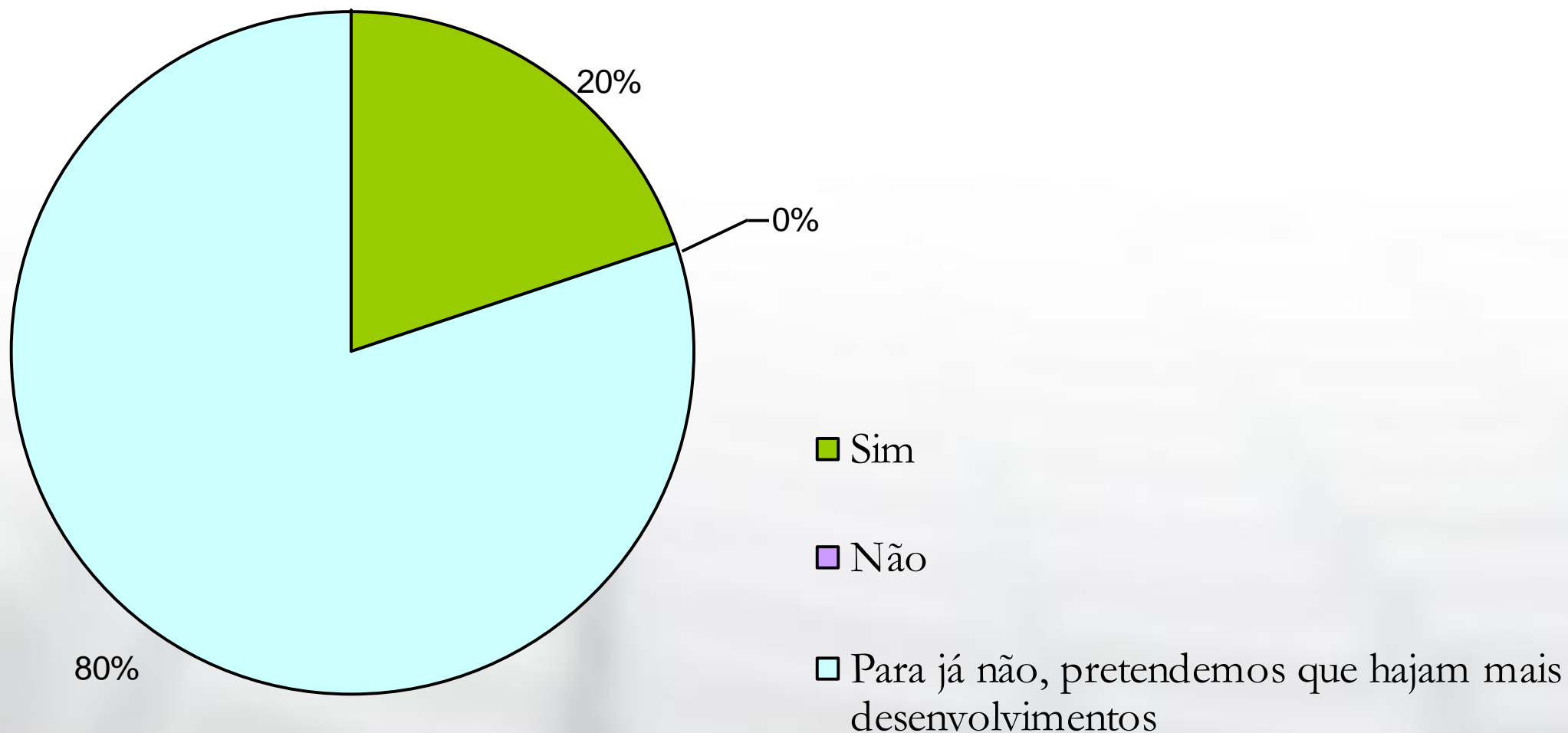
Considera a implementação de DNSSEC no ccTLD .PT uma mais valia para o serviço DNS?

- Sim
- Não sei, mas estou receptivo a mais informação
- Não



A sua entidade pretende adoptar este serviço?

A sua entidade pretende adoptar este serviço?



Estaria interessado em participar num Workshop Técnico para adquirir experiência prática na implementação de DNSSEC?

Estaria interessado em participar num Workshop Técnico para adquirir experiência prática na implementação de DNSSEC?

DEIXE-NOS O SEU CONTACTO!

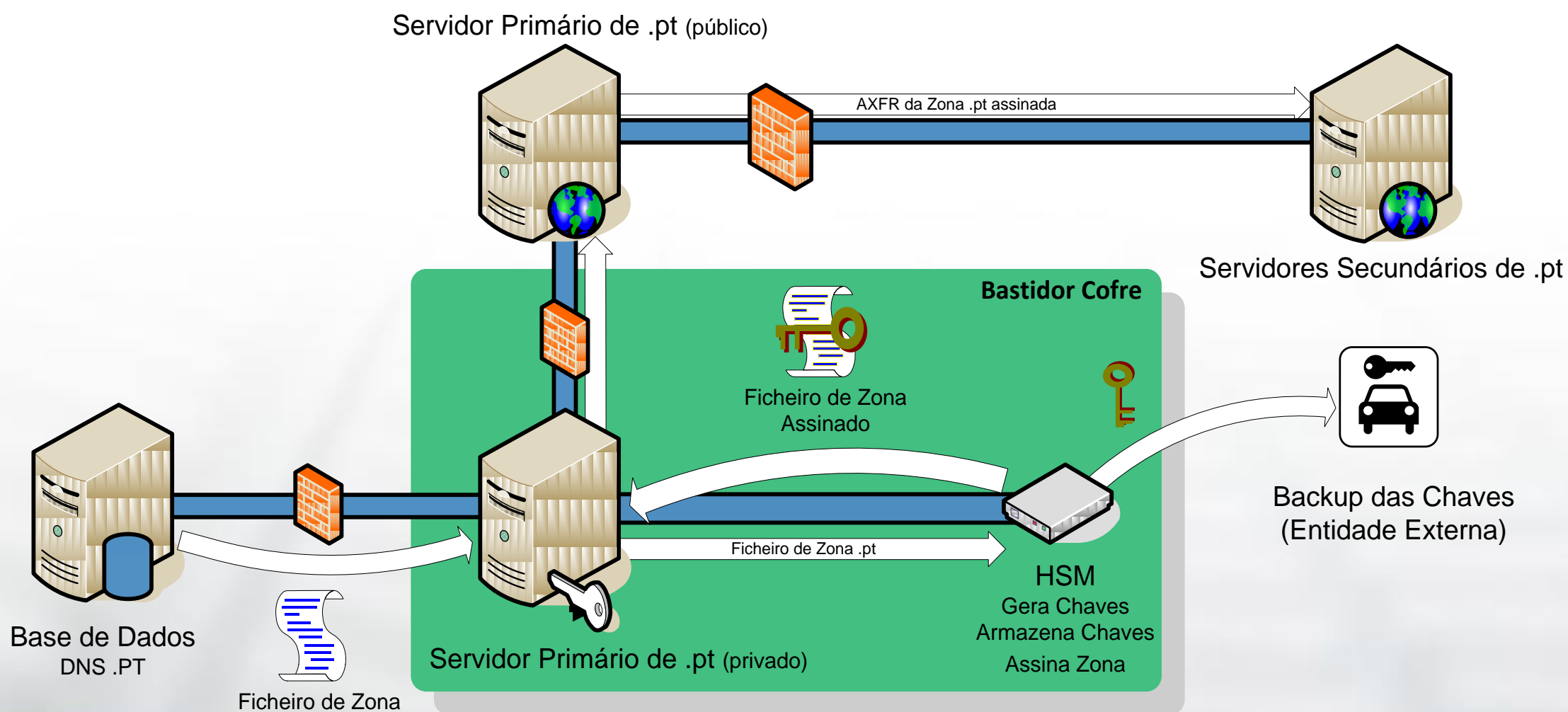
Cada vez existem mais ferramentas com suporte DNSSEC quer a nível de servidores como de aplicações, exemplos:

- BIND ISC (superior a 9.3.2)
- NSD, Unbound, ANS, CNS
- Sparta tools (logwatch, sendmail/postfix/libspf, dnsptkflow...)
- Mozilla/Firefox/Thunderbird plugins
- Windows Server 2008 R2 e Windows 7
- Para mais informação consulte:
 - <http://www.dnssec-deployment.org/tracker/>

Declaração de Política e Procedimentos:

- Documento de referência para avaliar o nível de confiança que o projecto DNSSEC do .pt confere às várias entidades intervenientes nos processos descritos
- Participantes e respectivas áreas de responsabilidade
- Procedimentos e esquemas operacionais relativos à implementação de DNSSEC pelo .pt
- Gestão e armazenamento das chaves da zona .pt
- Disponibilidade, confiança e integridade

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



dnssec.pt

- Domínio assinado (com NSEC3 Opt-Out, assina apenas os subdomínios com DNSSEC e evita a enumeração da zona *dnssec.pt*)
- Configurado no DLV do ISC
- Registo gratuito sob *dnssec.pt* para fins de teste
- Pedidos de registo submetidos para dev@dnssec.pt
- Mais informação disponível em:

<http://www.dnssec.pt>



- Domínio assinados cuja FCCN é titular:
 - dnssec.pt, fccn.pt, cert.pt, zappiens.pt, rcts.pt
- Cooperação com as Universidades para a assinatura dos domínios no âmbito da RCTS
- Lançamento de notícias e comunicados de imprensa
- Realização de Sessões de Divulgação
- Promoção de Workshops práticos
- Acções de Sensibilização

- Colocar em produção a zona .pt assinada
- Disponibilizar opções de gestão de DNSSEC no Sistema Online de Gestão de Domínios .pt
- Automatizar as alterações de Resource Records por meio de actualizações dinâmicas
- Integrar o DNSSEC no protocolo EPP

Obrigada pela vossa atenção



<http://www.dnssec.pt>

dev@dnssec.pt | info@dnssec.pt