LusNIC
Associação de ccTLDs de língua portuguesa

Coalition for Digital Africa

ICANN

DNSSEC

Workshop DNSSEC Prático

Assis Guerreiro, .PT
Engenheiro de Infraestruturas

23.02.2026

Agenda

1. Conceitos fundamentais de DNS/DNSSEC
2. Assinatura da zona DNS
3. Geração e configuração do registo DS
4. Validação DNSSEC
5. Rollover de chaves ZSK e KSK
6. Verificação e troubleshooting com Dig e DNSViz
7. Sessão de perguntas e respostas (Q&A)

Organização

09:00 – Início

10:30 – Cofee Break (10m)

12:00/13:00 – Almoço

14:30 – Cofee Break (10m)

15:30 – Fim da sessão

Requisitos recomendados para sessão:

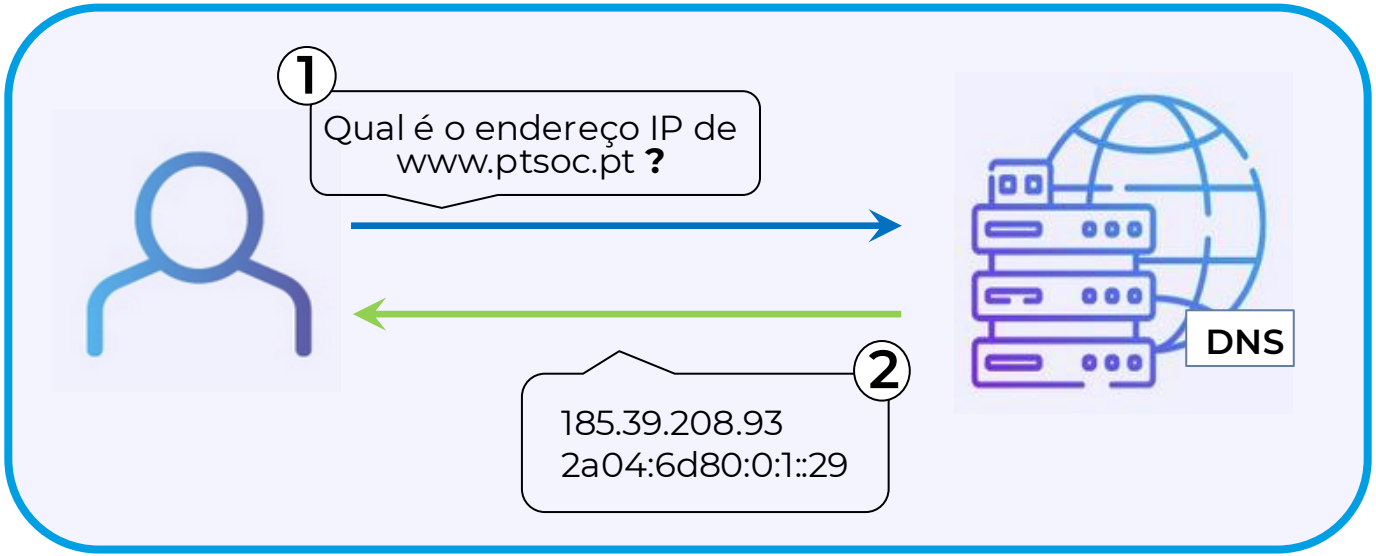
- Acesso à internet por browser
- Conhecimentos de básicos de DNS e redes
- Conhecimentos de Linux (linha de comandos)

O Serviço DNS

DNS

Domain Name System

Serviço de resolução de nomes de domínios legíveis e fáceis de memorizar em endereços IP e vice-versa.



O Serviço DNS

Componente fundamental e crítica da infraestrutura de suporte à Internet

O Serviço DNS

Resiliência

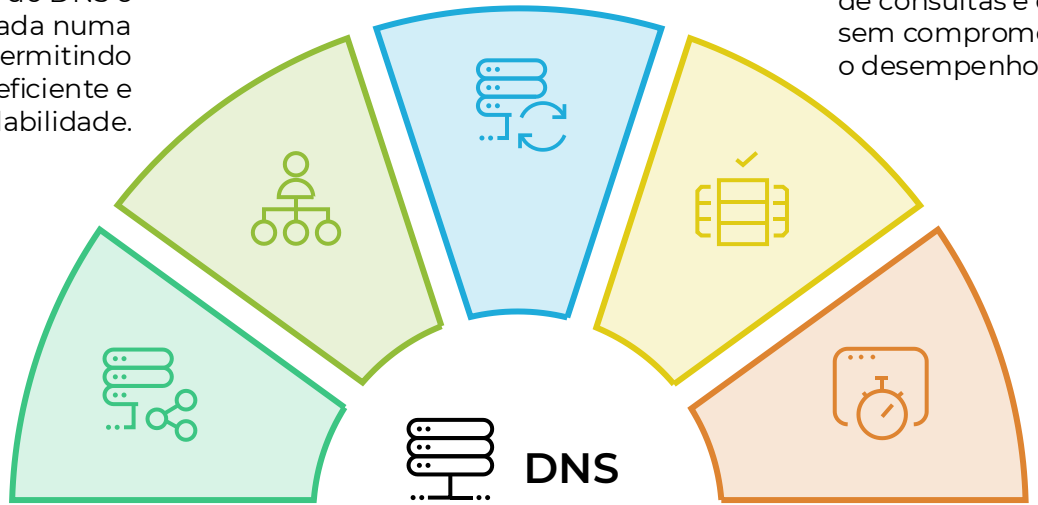
O DNS é projetado para resistir a falhas e manter a funcionalidade, garantindo uma operação contínua.

Hierárquica

A estrutura do DNS é organizada numa hierarquia, permitindo uma gestão eficiente e escalabilidade.

Escalabilidade

O DNS pode lidar com um número crescente de consultas e dispositivos sem comprometer o desempenho.



Distribuído

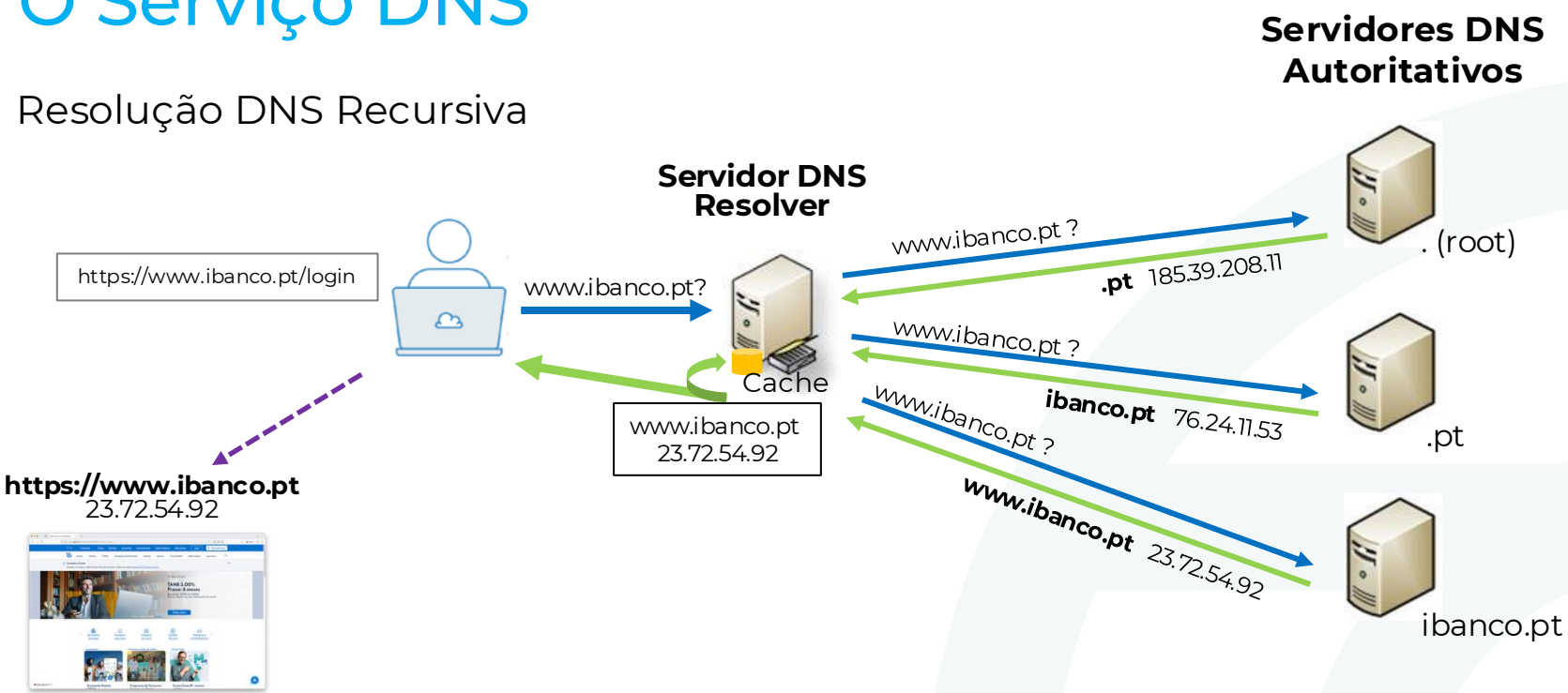
O DNS utiliza uma rede global de servidores, garantindo que nenhum ponto de falha possa comprometer o serviço.

Rapidez

O DNS fornece resolução rápida de nomes de domínio, garantindo acesso rápido a sites e serviços.

O Serviço DNS

Resolução DNS Recursiva



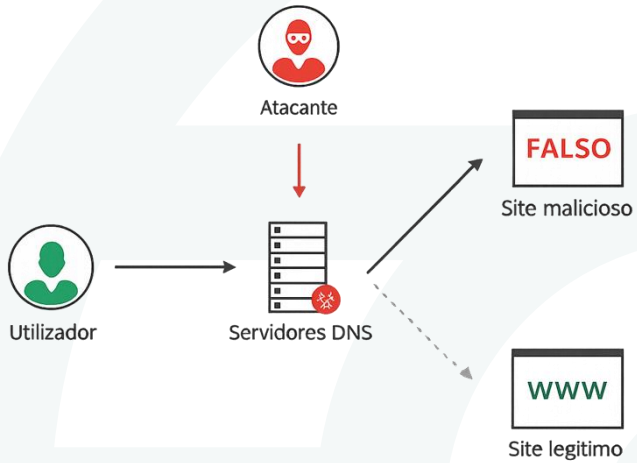
DNS: Vulnerabilidades

Insecure by design

O protocolo DNS foi desenvolvido sem mecanismos de segurança o que o torna o serviço DNS vulnerável a diversos tipos de ataques, nomeadamente:

DNS Spoofing, DNS Cache Poising, DNS Hijacking

- Redireccionamento para servidores de nomes/sites com fins maliciosos, controlados pelo atacante
  - Roubo de dados sensíveis de acesso a homebanking
  - Instalaçao de ransomware e malware



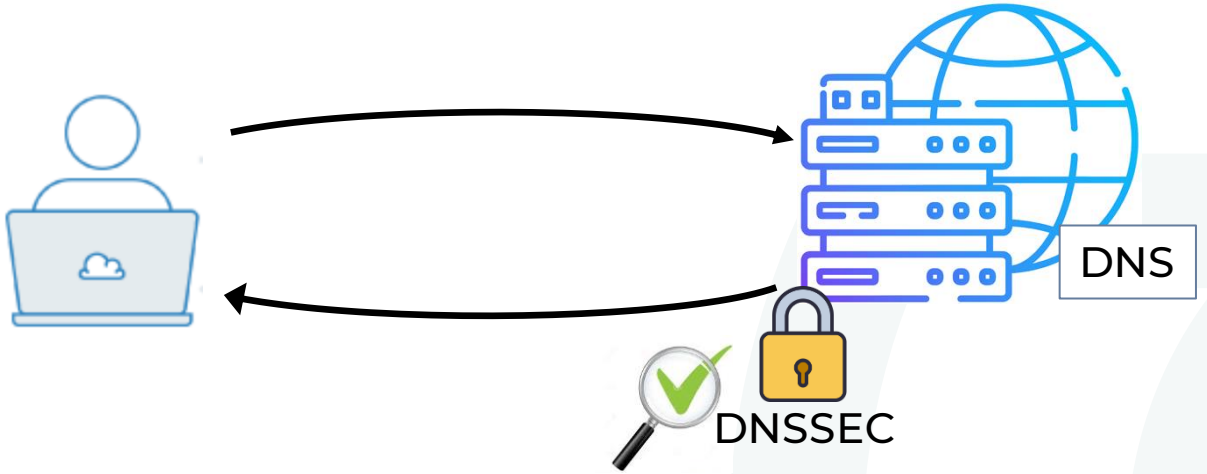
Daniel Kaminsky 2008
http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

DNSSEC

DNSSEC

Domain Name System Security Extensions

Extensões de segurança do protocolo DNS criadas para responder a ataques de Cache Poisoning / DNS Spoofing



DNSSEC

Características

- Evolução do serviço DNS
- A informação DNS é assinada e validada
- Transparente para utilizadores e sistemas
- Serviço DNS interoperável com/sem DNSSEC
- Gestão tendencialmente automática

DNSSEC

Integridade – garante que a informação DNS não é alterada em trânsito, desde que foi assinada na origem

Autenticidade – garante que a origem da informação DNS é legítima, e não de um atacante

Proof of Non-Existence – mesmo um "este domínio não existe" é verificável e não pode ser forjado - garante a integridade das respostas negativas

DNSSEC: SSL/TLS

Comparação entre SSL/TLS e DNSSEC

SSL/TLS	DNSSEC
Protege **comunicação** (HTTPS)	Protege **resolução** DNS
Usa **certificados** X.509	Usa **chaves** e **assinaturas**
Cadeia de confiança via CA	Cadeia de confiança via DS
Cifra a comunicação	**Não cifra** dados
Fornece **confidencialidade**	Fornece **integridade** e **autenticidade**

DNSSEC **não utiliza** certificados digitais !

Para privacidade, ***DoH*** *(DNS over HTTPS)* ou ***DoT*** *(DNS over TLS).*

DNSSEC: Novos registos

DNSKEY

Publica a **chave pública** da zona para validação de assinaturas.

RRSIG

Contém a **assinatura** digital de um RRset para garantir integridade.

DS

Publicado na zona pai, contém o hash da KSK da zona filha para **estabelecer a confiança**.

NSEC

Prova criptográfica de inexistência de registos para evitar respostas falsas.

NSEC3

Versão melhorada do NSEC que usa hashing para evitar zone walking.

Servidores e Resolução DNS

DNS Autoritativo vs DNS Recursivo

Comparando tipos de Servidores DNS por função

Servidores Autoritativos

Fonte da informação

Apenas responde o que tem configurado

Não faz cache

Assinam as zonas com DNSSEC

Procura a resposta completa

Navega pela hierarquia DNS

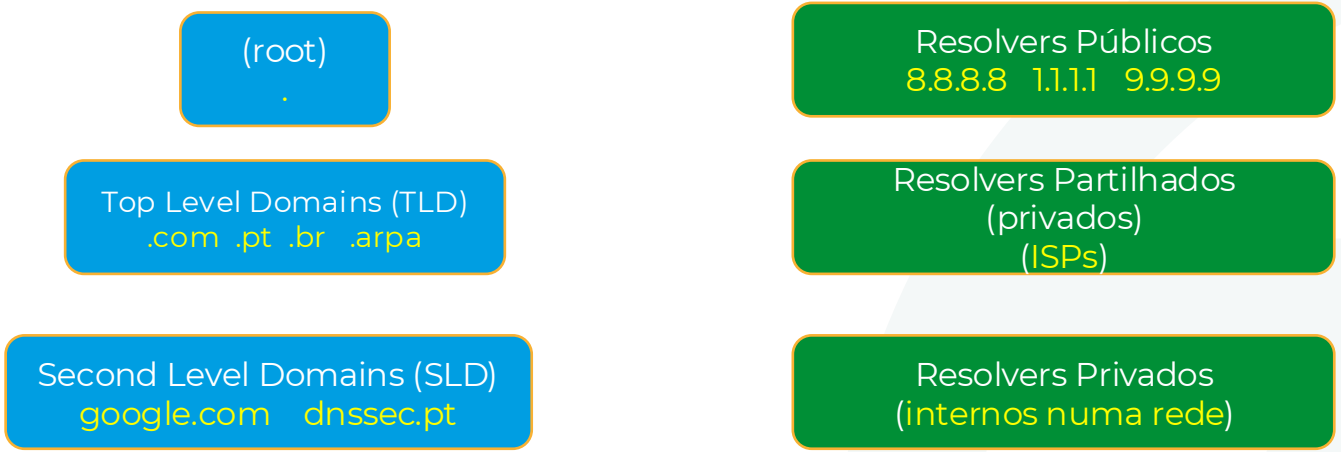
Guarda as respostas em cache

Validam as assinaturas DNSSEC

Resolvers (Recursivos)

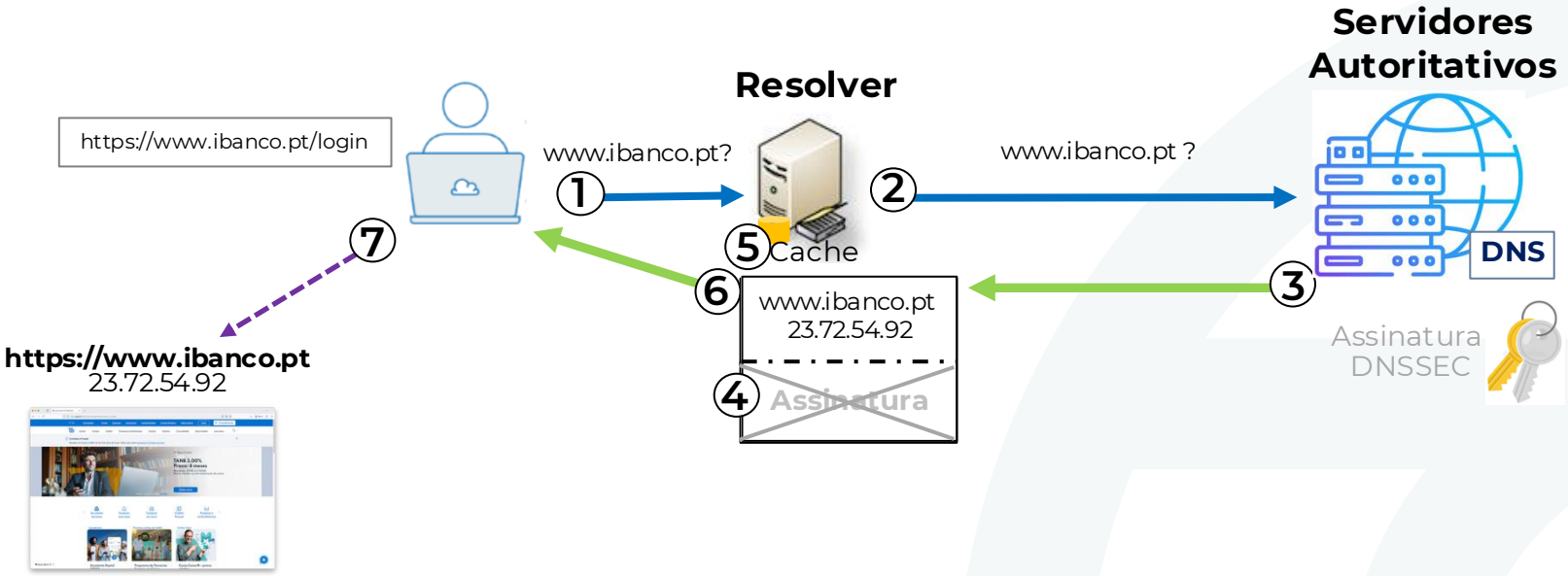
DNS Autoritativo vs Resolvers

Classificação de tipos de servidores por operadores



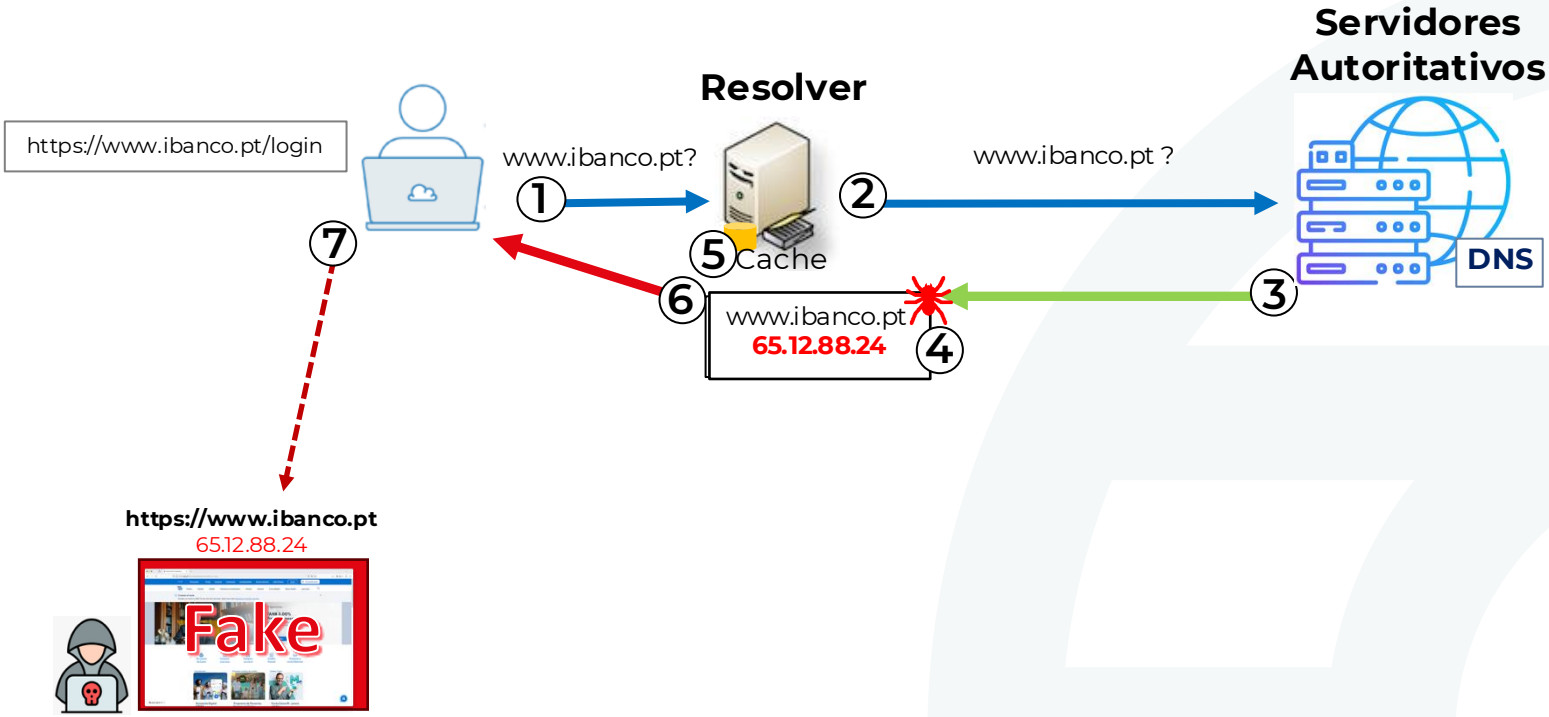
DNSSEC: Resolução DNS

Interoperabilidade DNSSEC



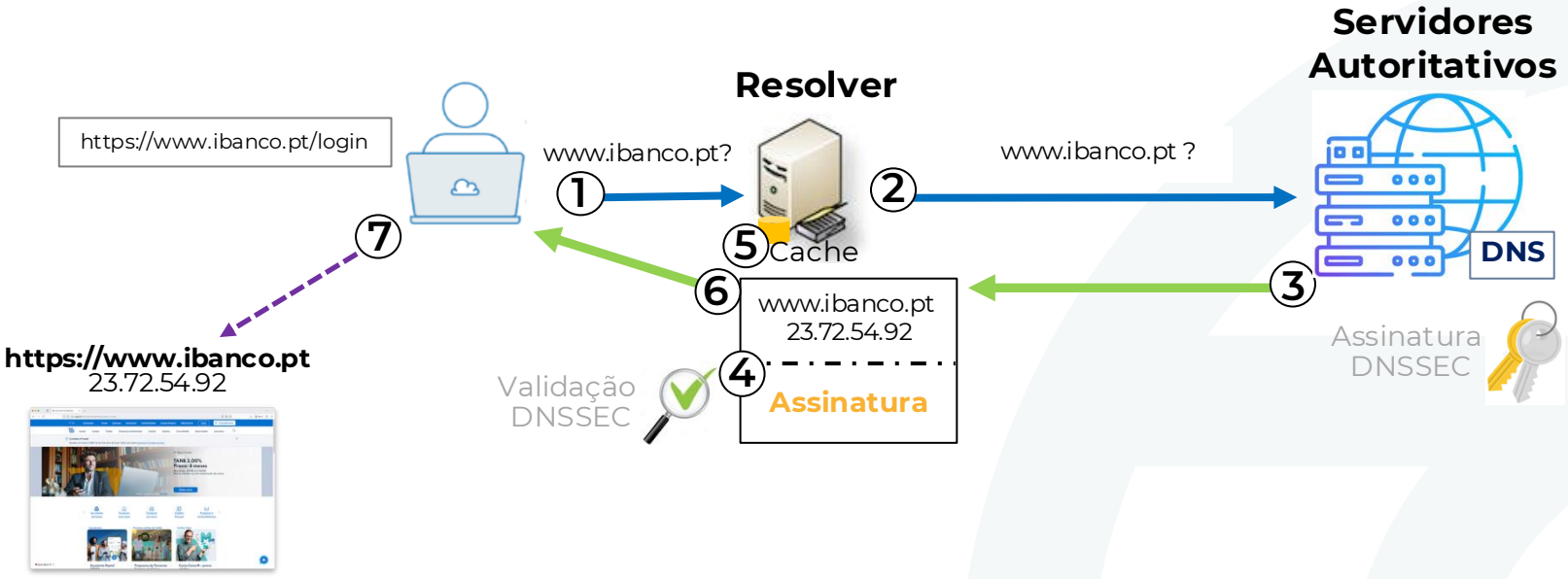
DNSSEC: Resolução DNS

Resolução DNS **sem DNSSEC**, ataque de **DNS Spoofing**



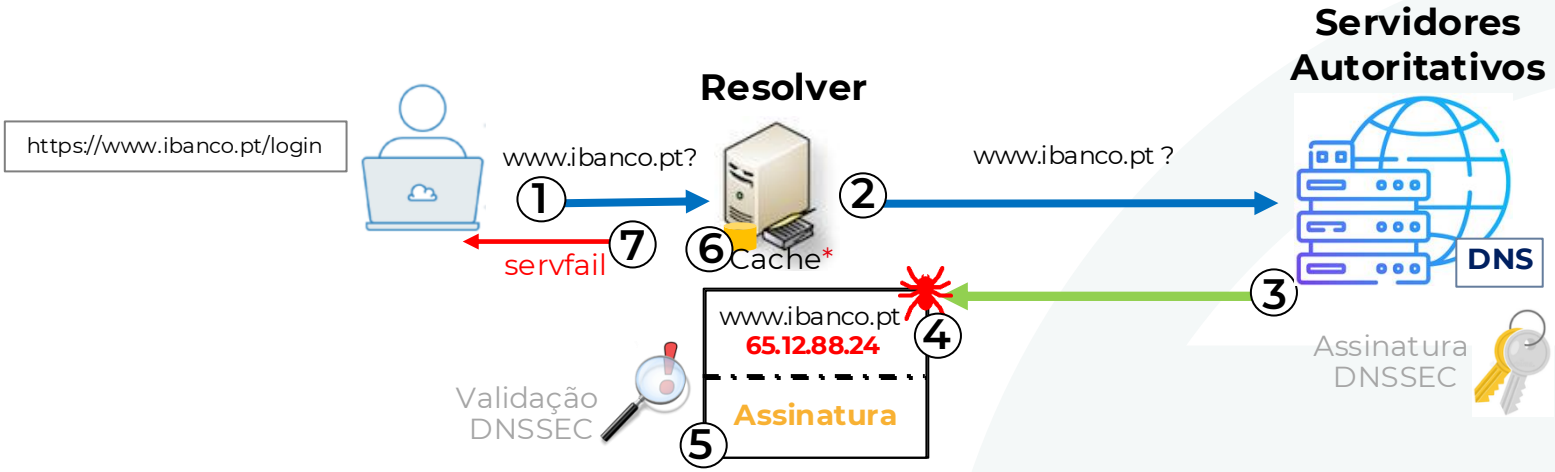
DNSSEC: Resolução DNS

Resolução DNS com validação DNSSEC



DNSSEC: servfail

Resolução DNS com DNSSEC, ataque de **DNS Spoofing**



*Negative Caching durante o TTL (último valor no SOA)

Chaves

DNSKEY

DNSSEC: Chaves

Qual é o aspeto de uma chave?

Chave Privada

```
# cat Kteste.pt.+013+58168.private
Private-key-format: v1.3
Algorithm: 13 (ECDSAP256SHA256)
PrivateKey: P/nxphwY+S/fS2A+LVcYObQsbdjBM6wGsMD4DgFpV+M=
```

Chave Pública

```
# cat Kteste.pt.+013+58168.key
; This is a key-signing key, keyid 58168, for teste.pt.
; Created: 20260219224206 (Thu Feb 19 22:42:06 2026)
; Publish: 20260219224206 (Thu Feb 19 22:42:06 2026)
; Activate: 20260219224206 (Thu Feb 19 22:42:06 2026)
teste.pt. IN DNSKEY 257 3 13 Qp/TRUhvzpy/5BHXzEYBS9G9dCinW1eZnrZhNguPkbpK0tWQaB1pSuhP
Foh3KewtagkTSNhjdAqJeO2ZJJh3dQ==
```

DNSSEC: Chaves

DNSSEC utiliza criptografia assimétrica (criptografia de chave pública)

🔑 Chave Privada → usada para assinar assinatura

🔑 Chave Pública → usada para validar a

Chave **ZSK** (Zone Signing Key)

- Publicada no registo **RRset DNSKEY**
- Assina os **RRsets da zona** (A, NS, MX, TXT, etc.)
- Utilizada sempre que a zona é assinada
- Rotação mais frequente

Chave **KSK** (Key Signing Key)

- Publicada no registo **RRset DNSKEY**
- Assina o **RRset DNSKEY**
- Referenciada na zona pai através do registo **DS**
- Elemento crítico da **cadeia de confiança**.
- Rotação menos frequente

É possível **conjugar** as funções das chaves **ZSK** e **KSK**, numa **única** chave

Chave **CSK** (Combined Signing Key)

DNSSEC: Chaves

KSK (Key Signing Key)

KSK
Privada

KSK
Pública

A chave KSK é utilizada para assinar e validar a chave ZSK, na cadeia confiança.

ZSK (Zone Signing Key)

ZSK
Privada

ZSK
Pública

A chave ZSK é utilizada para assinar e validar todos os registos DNS (RRs).

DNSSEC: Root Trust Anchor

Root **Trust Anchor** é a chave KSK pública da zona "." a raiz da Internet,

- Base da cadeia de confiança na validação DNSSEC
- Está pré-configurada nos Resolvers
- Resolvers suportam atualização automática via RFC 5011
- Gerida pela IANA/ICANN sob cerimónias criptográficas formais e altamente controladas

https://www.iana.org/dnssec/files

DNSSEC: Chaves

Propriedades das chaves DNSSEC

- Flags (ZSK/KSK/CSK)
- Algoritmo (RSA, ECDSA, Ed25519, etc.)
- Identificador (Key Tag / Key id)
- Tamanho da chave

```
;; ANSWER SECTION:
pt.                 3979 IN      DNSKEY 256 3 13 (
                                 0E6rLajHw7sAD01Eh/e1eo4e5O5JRnNiHdOTzDypmqPF
                                 KwInDIvpAH0BPCUOn9t3mlPdJ8/FxYyKMd9gqfHHzA==
                                 ) ; ZSK; alg = ECDSAP256SHA256 ; key id = 30640
pt.                 3979 IN      DNSKEY 257 3 13 (
                                 nfSs5LNsGhi3e4qjgY6KJxLxNHJahuEmEq2H1gLJHF4+
                                 bGZAm7BQwAbqFT3WJCgNqGlV2rEnBJn5DpQz4R4oAg==
                                 ) ; KSK; alg = ECDSAP256SHA256 ; key id = 40155
```

DNSSEC: Chaves

Algoritmos recomendados para gerar as chaves

Número	Descrição	Mnemonica	Estado
15	Ed25519	ED25519	⭐ Recomendado
13	ECDSA Curve P-256 with SHA-256	ECDSAP256SHA256	✅ Recomendado
8	RSA/SHA-256	RSASHA256	⚠️ Compatibilidade

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

DNSSEC: Rollover de chaves

As chaves DNSSEC **não** expiram!

Rollover de chaves é o processo de **substituir** as chaves activas por novas, mantendo a continuidade da **cadeia de confiança**. É uma operação delicada mas necessária por várias razões:

- **Política** de segurança da organização
- **Comprometimento** real ou suspeito da chave
- **Algoritmo** criptográfico obsoleto ou vulnerável

Assinaturas

RRSIG

DNSSEC: Assinaturas

As assinaturas DNSSEC são um **elemento critico**

- São utilizadas para a validação DNSSEC
- Têm sempre um período de **validade** pré-definido
- Início “Inception”, fim “Expiration” - YYYYMMDDHHMMSS (UTC)
- É preciso **reassinar**, dentro do período de validade
- As assinaturas e as chaves têm de **corresponder**

Problemas nas assinaturas, leva a falhas na validação DNSSEC

DNSSEC: Assinaturas

Características das assinaturas DNSSEC

- Criadas nos servidores autoritativos
- São geradas com a chave privada (**ZSK** ou **CSK**)
- São assinados conjunto de registos do mesmo tipo (**RRset**)
- Todos os registos RRset's na zona são assinados
- Publicadas nos registos RRs do tipo **RRSIG**

DNSSEC: Assinaturas

```
pt.          300  IN  SOA    curiosity.dns.pt. request.dns.pt. 2026022203 21600 7200 2592000 300
pt.          300  IN  RRSIG  SOA 13 1 7200 20260304005219 20260222005219 30640 pt.
rlCZOr38qwnliPLZGWzv8zgG/0pYKRDsak88sHutUa5BZoN2Q715D/tW 9YNJOkrqlJsvXPZAYHQ7ydbv1YrjlA==
```

RR do tipo RRSIG

Algoritmo Chave ZSK

TTL da zona

Expiration Date
2026/03/04 00:52:19

Inception Date
2026/02/22 00:52:19

ZSK KeyTag Id

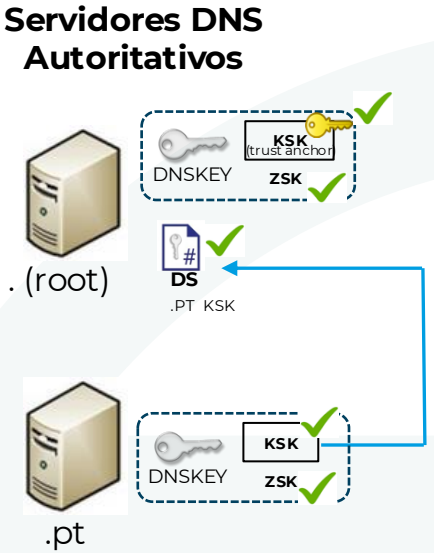
Delegation Signer

DS

DNSSEC: DS

O registo *delegation signer* (DS) é o **elo de ligação** entre hierarquias DNS

- É um **hash** da **KSK pública** da zona abaixo
- É gerada pelo servidor autoritativo da zona abaixo
- Tem de **corresponder** à chave KSK



O registo DS estabelece a confiança na hierarquia abaixo!

DNSSEC: DS

Algoritmos recomendados para gerar os registos DS

Número	**Descrição**
2	SHA-256

Fonte: https://datatracker.ietf.org/doc/html/rfc9904 - name-digest-algorithms-registry-

DNSSEC: DS

Na zona root

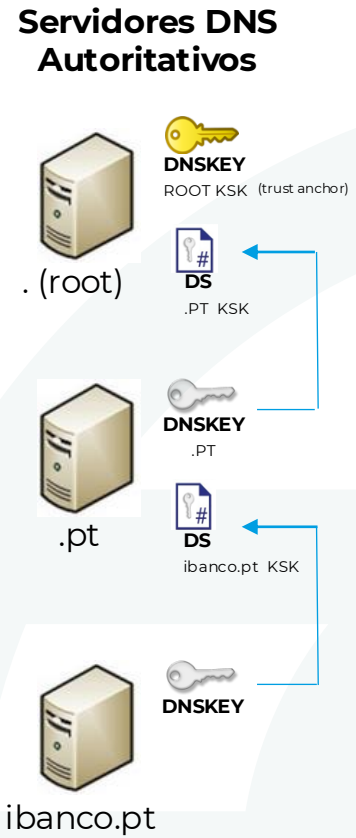
```
pt.                 86400       IN      DS      40155 13 2
B0ED28B7255E9880E7CE4665B75AE7271F7837899057F0D4B897ECE2 EB1EB494
```

Na zona .pt

```
pt.                 3130 IN     DNSKEY 256 3 13 (
                                0E6rLajHw7sAD01Eh/e1eo4e5O5JRnNiHdOTzDypmqPF
                                KwInDlvpAH0BPCUOn9t3mlPdJ8/FxYyKMd9gqfHHzA==
                                ) ; ZSK; alg = ECDSAP256SHA256 ; key id = 30640
pt.                 3130 IN     DNSKEY 257 3 13 (
                                nfSs5LNsGhi3e4qjgY6KJxLxNHJahuEmEq2H1gLJHF4+
                                bGZAm7BQwAbqFT3WJCgNqGlV2rEnBJn5DpQz4R4oAg==
                                ) ; KSK; alg = ECDSAP256SHA256 ; key id = 40155
pt.                 3130 IN     RRSIG DNSKEY 13 1 7200 (
                                20260315000000 20260125000000 40155 pt.
                                jdeWxRASYL5JEQjykg53XqHlpjDTtSpwsCs73m7QQS+x
                                cdVLCzzAnXRDqOHVBstMc03FBIwqVkjdWeVMcVYVsg== )
```

DNSSEC: DS

A metodologia de estabelecimento de **confiança** entre zonas **repete-se** ao longo de todos os servidores autoritativos na hierarquia que faz parte da resolução de um dado domínio.

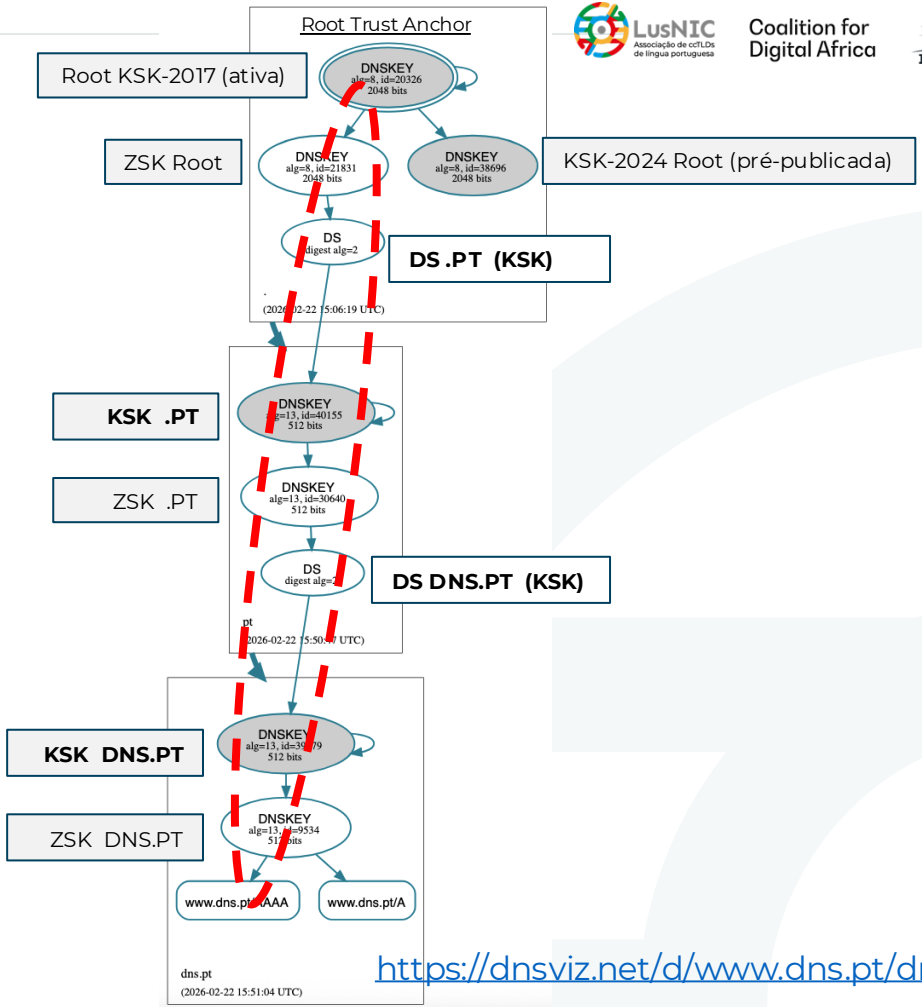


Validação

DNSSEC: Validação

No processo de validação, os servidores Resolver **percorrem a hierarquia** DNS desde da raiz até ao domínio que está a ser validado.

Esta sequência de validações completa, é uma **cadeia de confiança hierárquica** conhecida por “chain of trust”



https://dnsviz.net/d/www.dns.pt/dnssec/

DNSSEC: Validação

As resposta DNS validadas com DNSSEC são assinaladas com a flag AD (Authentic Data)

```
; <<>> DiG 9.10.6 <<>> @8.8.8.8 dnssec.pt ns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21631
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;dnssec.pt.                     IN      NS

;; ANSWER SECTION:
dnssec.pt.              900     IN      NS      dns02.dns.pt.
dnssec.pt.              900     IN      NS      dns01.dns.pt.
```

dig dns.pt +trace +dnssec

DNSSEC: Validação

Também é possível observar a validação DNSSEC com a ferramenta delv (BIND tools)

```
$ delv  mail01.dns.pt
; fully validated
mail01.dns.pt.          134     IN      A       185.39.208.66
mail01.dns.pt.          134     IN      RRSIG   A 13 3 300 20260318020021 20260216020021
9534 dns.pt. bKA695VvUcguE+BCqfNQLVJzJZU+9LyPsnvHHze8gMTY0yCkrKFJOnnh
01UfM0NkLJg7/Foi2+fFOsZ9kc3ePg==
```

delv +rtrace dns.pt	lista os domínios incluídos no processo de validação
delv +vtrace dns.pt	detalhe do processo de validação

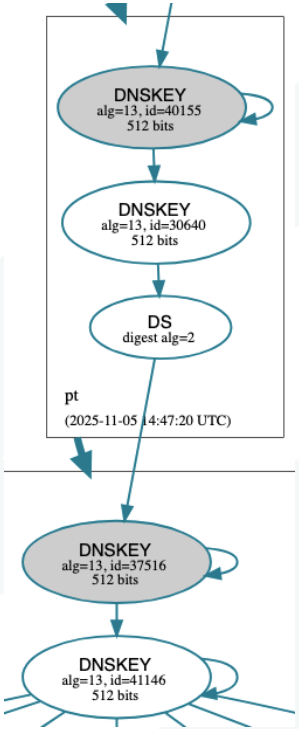
DNSSEC

Pode existir **uma ou várias** chaves KSK e respetivos registos DS.

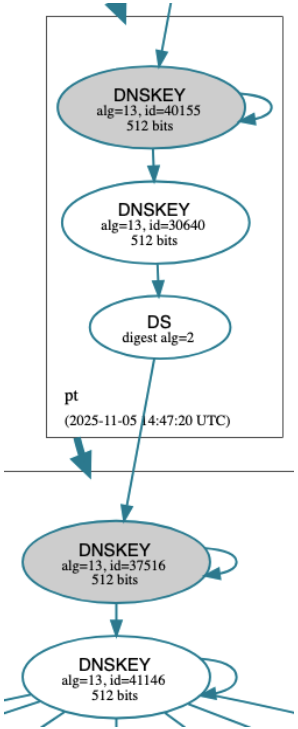
A validação DNSSEC necessita de **pelo menos** uma correspondência válida.

Este cenário é comum quando ocorre um Rollover da chave KSK.

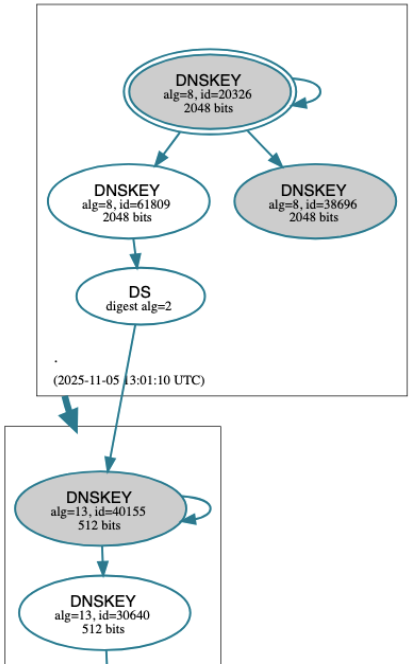
Durante esta fase, as repostas DNS são **maiores**, o que pode promover ataques de amplificação.



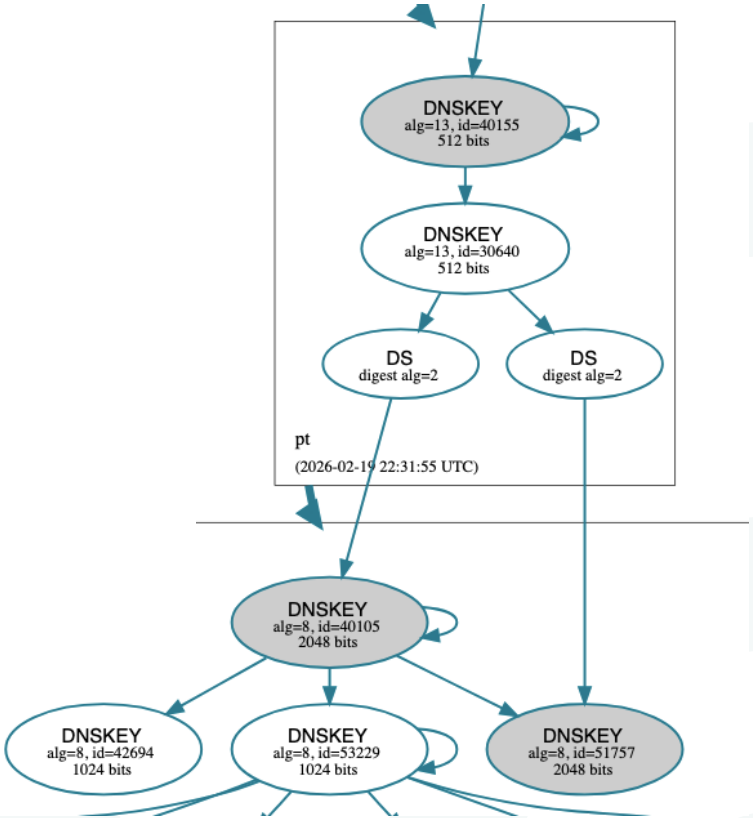
DNSSEC



Cenário A



Cenário B



Cenário C

DNSSEC: Implementar

Possíveis etapas para implementar DNSSEC

- Adquirir conhecimentos
- Definir parâmetros das chaves e assinaturas
    - Algoritmos, validade das assinaturas, Rollovers
- Gerar as chaves KSK/ZSK ou CSK
- Salvaguardar as chaves em local seguro

DNSSEC: Implementar

- Assinar zona de testes
- Rever
- Documentar procedimentos
- Assinar
- Validar e Monitorizar

DNSSEC: Bind

O software BIND permite implementar DNSSEC com alguns automatismos.

- Assinar e atualizar as assinaturas automaticamente;
- Gestão das chaves
- Parametrizações NSEC

```
zone "example.com" {
    type primary;
    file "example.com.zone";
    dnssec-policy "default"; // Enables automatic DNSSEC
};
```

https://kb.isc.org/docs/dnssec-key-and-signing-policy

DNSSEC: Bind “default”

```
dnssec-policy "default" {
        keys {
                csk key-directory lifetime unlimited algorithm ecdsa256;
        };
        ...
        # Key timings
        dnskey-ttl PT1H;
        publish-safety PT1H;
        retire-safety PT1H;
        purge-keys P90D;
        ...
        # Signature timings
        signatures-refresh P5D;
        signatures-validity P14D;
        signatures-validity-dnskey P14D;
        ...
        # Zone parameters
        max-zone-ttl P1D;
        zone-propagation-delay PT5M;
        parent-ds-ttl P1D;
        parent-propagation-delay PT1H;
};
```

https://kb.isc.org/docs/dnssec-key-and-signing-policy

DNSSEC: Bind

Customização da política de automatismos do software BIND.

- Definir as chaves;
- Definir os parâmetros de Rollover

```
dnssec-policy "myway" {
        keys {
                ksk lifetime unlimited algorithm rsasha256 2048;
                zsk lifetime P60D algorithm rsasha256 1024;
        };
};
...
zone "example.com" {
        dnssec-policy myway;
};
```

https://kb.isc.org/docs/dnssec-key-and-signing-policy

DNSSEC: possíveis problemas

Situações de problemas que podem afetar a validação DNSSEC, e soluções

- Assinaturas expiradas
  - ✓ A zonas tem ser assinadas sempre que são alteradas, ou regularmente mesmo que não sejam alteradas.
- Registo DS não corresponder à chave KSK
  - ✓ Garantir sempre pelo menos uma correspondência entre o registo DS e a respetiva chave KSK
- Zona incompleta sem o RRset DNSKEY, as chaves KSK/ZSK
  - ✓ Gerar nova zona com o RRset DNSKEY

DNSSEC: possíveis problemas

- Chaves ou registos DS retirados cedo demais antes
  - ✓ Devem ser respeitados os tempos da informação em cache nos Resolvers
- Dessincronização do relógio entre servidores Resolvers e Autoritativos
  - ✓ Deve ser usado NTP para sincronizar nos vários servidores
- Utilização de Algoritmos fracos
  - ✓ Deve ser realizado um rollover com a introdução de algoritmos recomendados e mais robustos

DNSSEC: boas práticas

Sugestões de boas práticas para implementar DNSSEC em TLDs ou domínios de relevo

- Adquirir conhecimentos sólidos
- Devem ser utilizados servidores específicos para cada função das zonas DNS: gerar/assinar/publicar/disponibilizar
- Validar, validar, validar….
- Monitorizar as assinaturas para evitar que expirem

DNSSEC: boas práticas

- Monitorizar as assinaturas para evitar que expirem
- Utilizar software atualizado
- Salvaguardar chaves KSK em local seguro
- Utilizar ferramentas para diagnosticar possíveis falhas
- Criar uma plataforma de testes
- Divulgar e dar apoio a comunidade Internet local na forma de workshops e uma linha (email/chat) de suporte/esclarecimentos.

DNSSEC: Ferramentas

Alguns ferramentas de análise DNS/DNSSEC

DNSVIZ - visualização gráfica da cadeia de confiança DNSSEC
https://dnsviz.net/

Verisign Labs *DNSSEC Analyzer* - análise rápida da cadeia DNSSEC
https://dnssec-analyzer.verisignlabs.com/

Zonemaster - testa a qualidade e conformidade de uma zona DNS, com foco em DNSSEC
https://zonemaster.net/en/

DNSSEC: RFC’s

Alguns RFC’s com especificações DNSSEC

RFC 4033	DNS Security Introduction and Requirements
RFC 4034	Resource Records for DNS Security Extensions
RFC 4035	Protocol Modifications for DNS Security Extensions
RFC 6840	Clarifications and Implementation Notes for DNS Security
RFC 7583	DNSSEC Key Rollover Timing Considerations
RFC 6781	DNSSEC Operational Practices, Version 2
RFC 9364	DNS Security Extensions (DNSSEC) — BCP 237
RFC 8499	DNS Terminology

LusNIC
Associação de ccTLDs de língua portuguesa

Coalition for Digital Africa

ICANN

OBRIGADO!

lusnic@lusnic.org