

Tutorial DNSSEC ¹

Cesar Henrique Kuroiwa
<tutorial-dnssec@registro.br>

Registro.br

3 de maio de 2012

¹ versão 1.7.4 (Revision)
A última versão deste tutorial pode ser encontrada em: <ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf>

- Introduzir os conceitos de DNS e DNSSEC
- Apresentar um exemplo prático de DNSSEC utilizando BIND
- Incentivar a utilização de DNSSEC

1 Introdução DNS

- Conceitos
- Publicação
- Arquitetura
- Softwares
- Vulnerabilidades

2 DNSSEC

- Conceitos
- Resource Records
- Funcionamento
- DNS vs DNSSEC
- Softwares

3 DNSSEC na Prática

- DNSSEC no Servidor Autoritativo
- DNSSEC no Servidor Recursivo

4 Referências

Parte I

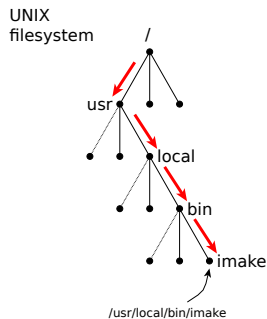
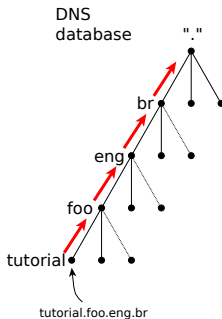
Introdução DNS

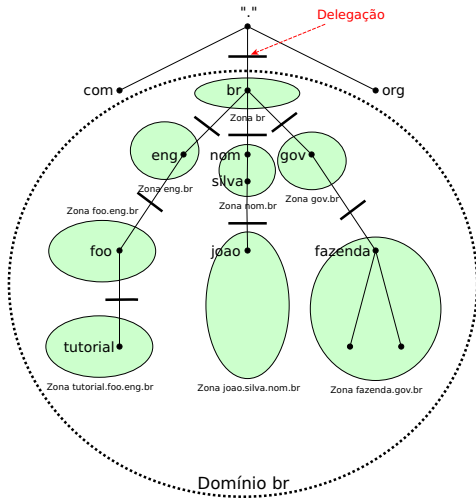


O Sistema de Nomes de Domínio é um banco de dados distribuído. Isso permite um controle local dos segmentos do banco de dados global, embora os dados em cada segmento estejam disponíveis em toda a rede através de um esquema cliente-servidor.

- Arquitetura hierárquica, dados dispostos em uma árvore invertida
- Distribuída eficientemente, sistema descentralizado e com cache
- O principal propósito é a resolução de nomes de domínio em endereços IP e vice-versa

exemplo.foo.eng.br	↔	200.160.10.251
www.cgi.br	↔	200.160.4.2
www.registro.br	↔	2001:12ff:0:2::3





Delegação

Indica uma transferência de responsabilidade na administração a partir daquele ponto na árvore DNS

Zona

Parte do sistema de domínios com informações e administração locais (ex: eng.br e foo.eng.br)

- Reserva o direito da pessoa física ou jurídica sobre um determinado nome de endereço na Internet.
- Inclui uma nova delegação para o domínio abaixo da zona .br.
- Domínios não registrados não podem ser encontrados na Internet.

Sistema WEB

A interface WEB permite de maneira prática gerenciar os domínios de qualquer pessoa física ou jurídica.

– <http://registro.br/suporte/tutoriais/novo-registro.html>

EPP - Extensible Provisioning Protocol

É uma interface destinada somente a provedores de serviço previamente certificados pelo Registro.br.

– <http://registro.br/epp/>

O que é uma Publicação?

As modificações que são realizadas pela interface não são efetivadas imediatamente. A cada intervalo de tempo pré-determinado ocorre uma publicação DNS, a qual atualiza as informações públicas na internet.

O que é uma Publicação?

As modificações que são realizadas pela interface não são efetivadas imediatamente. A cada intervalo de tempo pré-determinado ocorre uma publicação DNS, a qual atualiza as informações públicas na internet.

As publicações DNS ocorrem a cada 30 minutos

- No caso do registro de um novo domínio ele já estará visível na Internet após a próxima publicação.
- No caso da alteração de dados de um domínio, após a próxima publicação, o domínio passará por um período de transição que poderá durar até 24 horas (tempo necessário para que o TTL do domínio expire e elimine o cache).

Os dados associados com os nomes de domínio estão contidos em **Resource Records** ou **RRs** (Registro de Recursos)

- São compostos por nome, classe, tipo e dados
- Atualmente existe uma grande variedade de tipos
- O conjunto de resource records com o mesmo nome de domínio, classe e tipo é denominado **Resource Record Set (RRset)**

Alguns Tipos Comuns de Records

SOA Indica onde começa a *autoridade* a zona

NS Indica um *servidor de nomes* para a zona

A Mapeamento de nome a endereço (IPv4)

AAAA Mapeamento de nome a endereço (IPv6)

MX Indica um *mail exchanger* para um nome (servidor de email)

CNAME Mapeia um nome alternativo (apelido) Apêndice II - CNAME

Arquivo de zona - Possui os RRs referentes a um determinado domínio, sendo que cada domínio possui um arquivo de zona.

```
exemplo.com.br. IN SOA ns1.exemplo.com.br. hostmaster.exemplo.com.br. (  
    1          ; serial  
    3600       ; refresh  
    3600       ; retry  
    3600       ; expire  
    900 )      ; minimum
```

Apêndice I - SOA

```
exemplo.com.br.          IN NS ns1.exemplo.com.br.  
exemplo.com.br.          IN NS ns2.exemplo.com.br.  
ns1.exemplo.com.br.      IN A 10.0.0.1  
ns2.exemplo.com.br.      IN A 10.0.0.2  
  
exemplo.com.br.          IN MX 10 mail.exemplo.com.br.  
mail.exemplo.com.br.     IN A 10.0.0.3  
  
www.exemplo.com.br.      IN A 10.0.0.4
```

Ferramentas recomendadas para consultas sobre registros de DNS de um determinado domínio, host ou IP:

- DIG (Domain Information Groper)
 - <http://www.isc.org/software/bind>
- DRILL
 - <http://www.nlnetlabs.nl/projects/drill>

	Criador	Código Aberto	Grátis
ANS	Nominum		
BIND	Internet System Consortium	✓	✓
djbdns	Daniel J. Bernstein	✓	✓
DNSSHIM	Registro.br	✓	✓
IPControl	INS		
IPM DNS	EfficientIP		
MaraDNS	Sam Trenholme	✓	✓
Microsoft DNS	Microsoft		
NSD	NLnet Labs	✓	✓
PowerDNS	PowerDNS.com / Bert Hubert	✓	✓
Unbound	NLnet Labs	✓	✓
Vantio	Nominum		
VitalQIP	Lucent Technologies		

	BSD ^a	Solaris	Linux	Windows	MAC OS X
ANS	✓	✓	✓		
BIND	✓	✓	✓	✓	✓
djbdns	✓	✓	✓		✓
DNSSHIM	✓	✓	✓	✓	✓
IPControl		✓	✓	✓	
IPM DNS	✓	✓	✓		✓
MaraDNS	✓	✓	✓	✓ ^b	✓
Microsoft DNS				✓	
NSD	✓	✓	✓		✓
PowerDNS	✓	✓	✓	✓	✓ ^c
Unbound	✓	✓	✓		✓
Vantio	✓	✓	✓		
VitalQIP		✓	✓	✓	

^a Sistema compatível com a norma POSIX assim como outros clones do Unix.

^b Apenas nas versões mais recentes do sistema operacional

^c Software em versão Beta

Servidor Autoritativo

- Responde com autoridade para uma zona específica
- Deve estar disponível publicamente para toda a internet

Servidor Recursivo

- Não é responsável por uma única zona
- Ao receber uma requisição, consulta servidores autoritativos para obter a informação desejada
- Faz cache de informações
- Pode ter acesso controlado

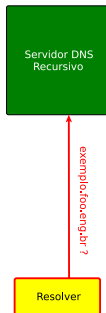
Supondo que o
cache está vazio ou
sem informações de
br, eng.br,
foo.eng.br,
exemplo.foo.eng.br

Resolver

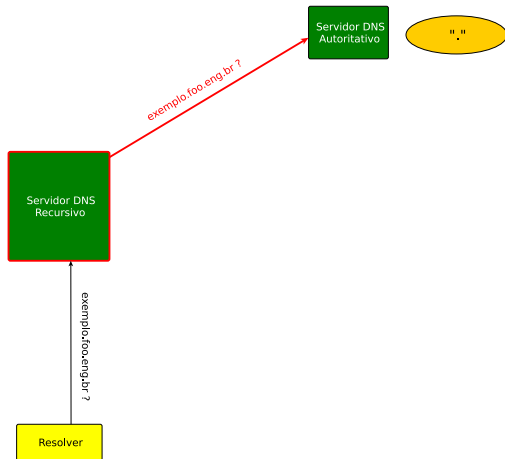
Serviço localizado
no cliente que tem
como
responsabilidade
resolver as
requisições DNS
para diversos
aplicativos

Resolver

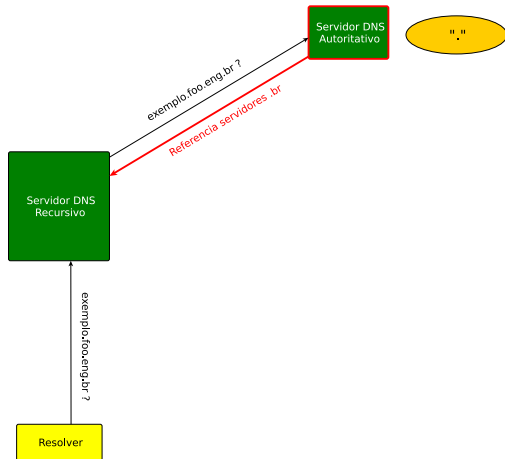
Supondo que o
cache está vazio ou
sem informações de
br, eng.br,
foo.eng.br,
exemplo.foo.eng.br



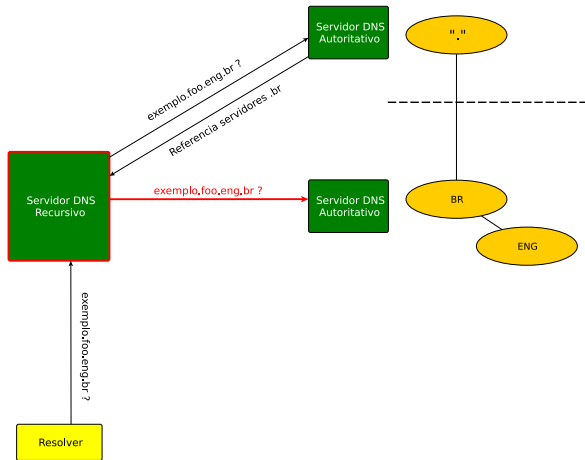
Exemplo de requisição de endereço



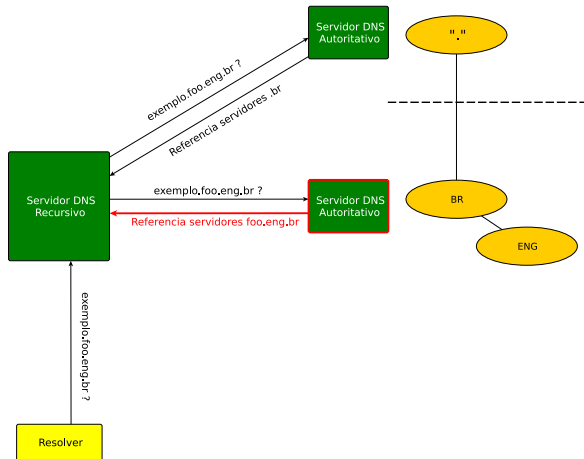
Exemplo de requisição de endereço



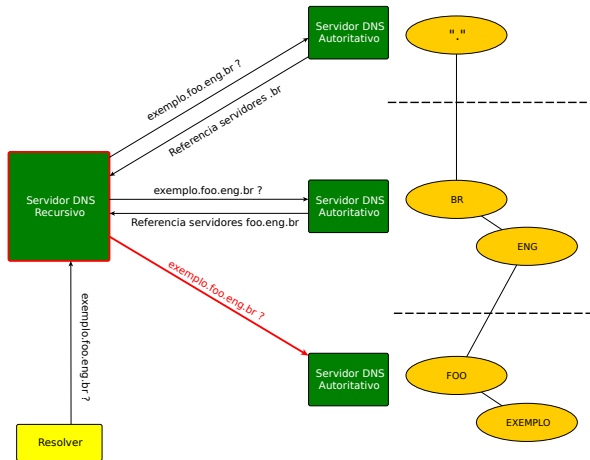
Exemplo de requisição de endereço



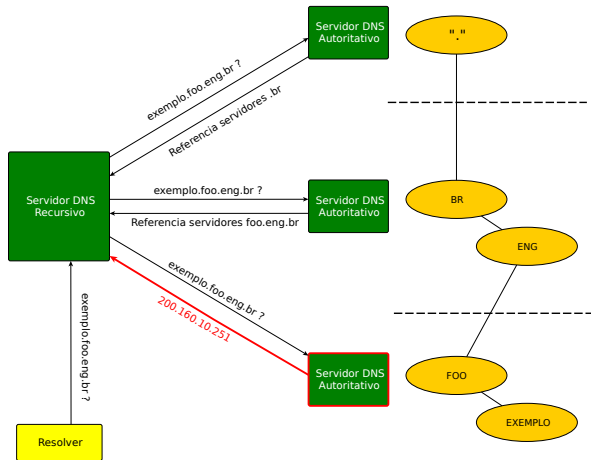
Exemplo de requisição de endereço



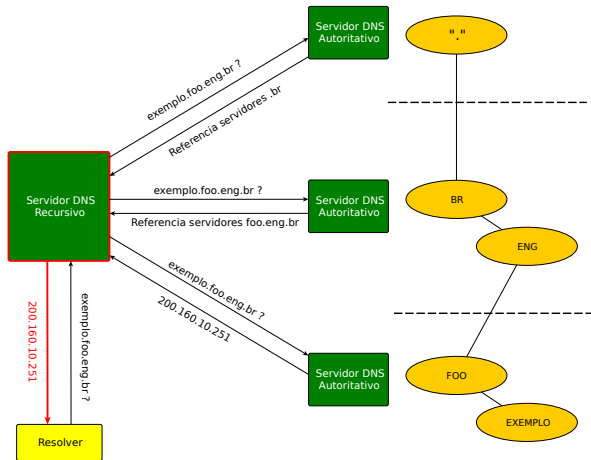
Exemplo de requisição de endereço



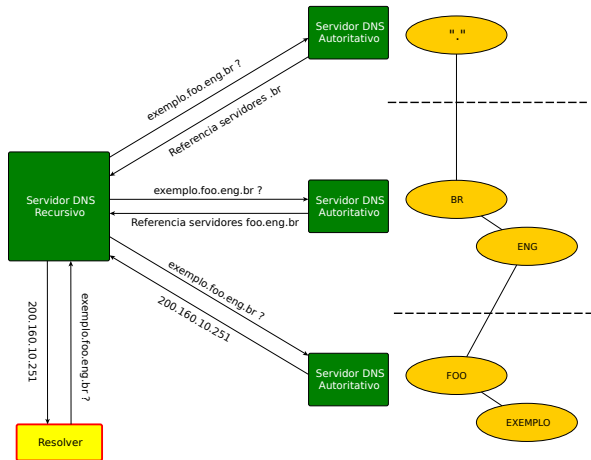
Exemplo de requisição de endereço

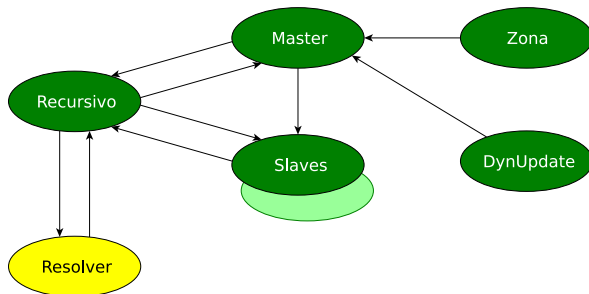


Exemplo de requisição de endereço

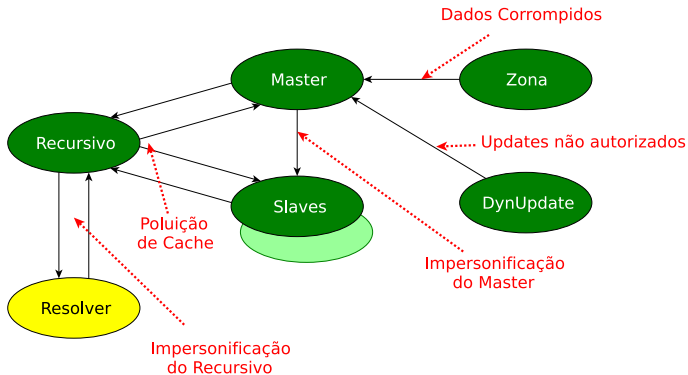


Exemplo de requisição de endereço





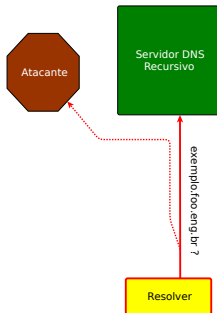
- 1 Resolver faz consultas no Recursivo
- 2 Recursivo faz consultas no Master ou Slave
- 3 Master tem a zona original (via arquivo ou Dynamic Update)
- 4 Slave recebe a zona do Master (AXFR ou IXFR)



Man-in-The-Middle

Exemplo de Ataque 1

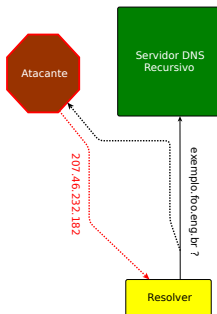
Man-in-The-Middle



Exemplo de Ataque 1

Man-in-The-Middle

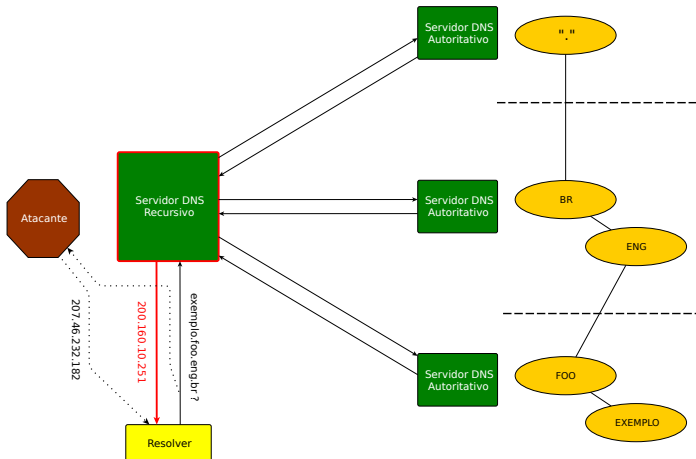
O atacante responde mais rápido, spoofando endereço do recursivo



Exemplo de Ataque 1

Man-in-The-Middle

O atacante responde mais rápido, spoofando endereço do recursivo



Exemplo de Ataque 2

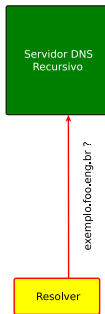
Poluição de Cache



Resolver

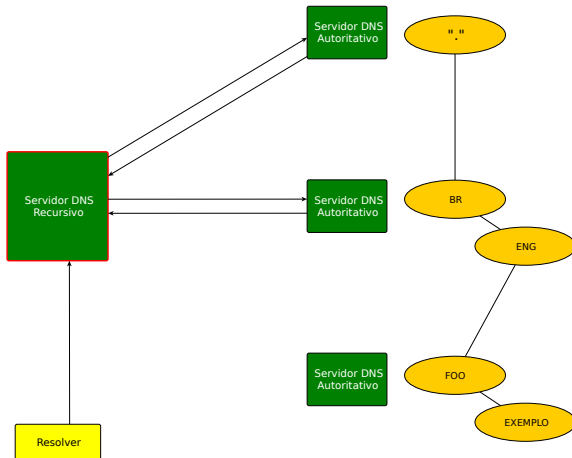
Exemplo de Ataque 2

Poluição de Cache



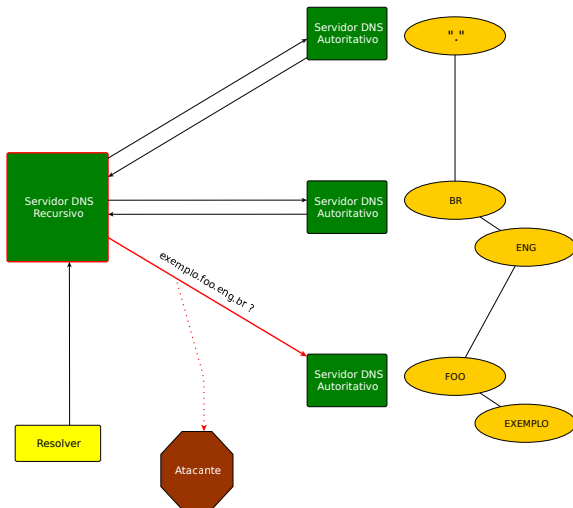
Exemplo de Ataque 2

Poluição de Cache



Exemplo de Ataque 2

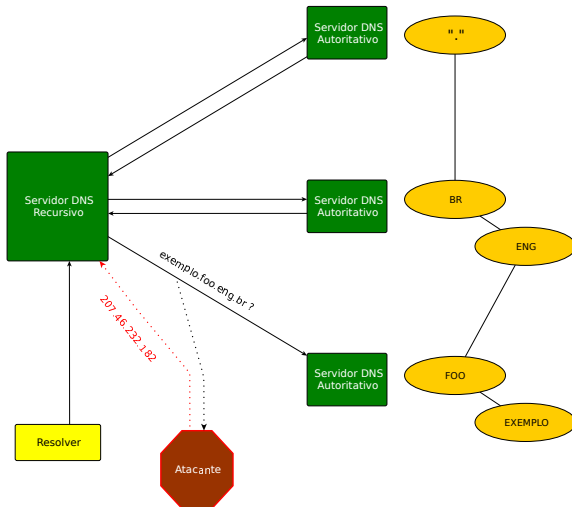
Poluição de Cache



Exemplo de Ataque 2

Poluição de Cache

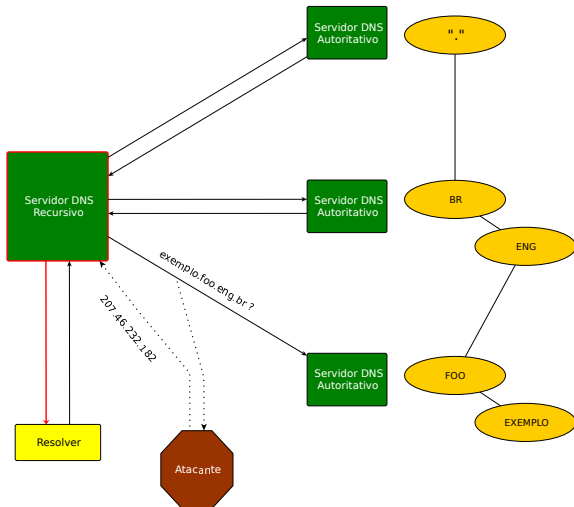
O atacante responde mais rápido, spoofando endereço do autoritativo



Exemplo de Ataque 2

Poluição de Cache

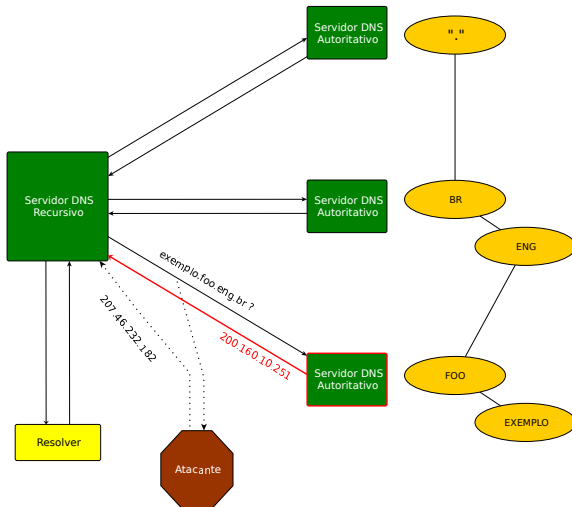
O atacante responde mais rápido, spoofando endereço do autoritativo



Exemplo de Ataque 2

Poluição de Cache

O atacante responde mais rápido, spoofando endereço do autoritativo



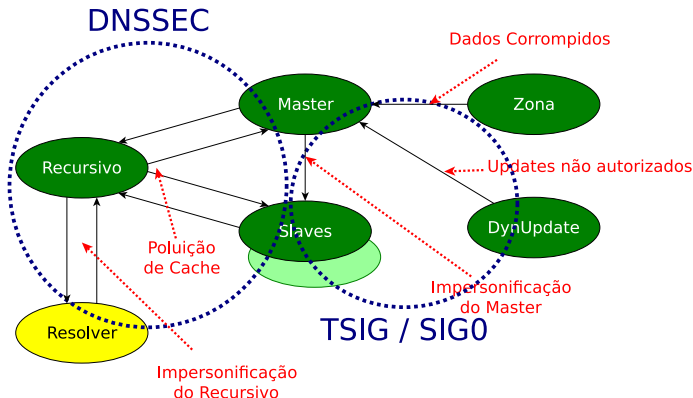
Segmentos compartilhados L2 ponto-multiponto

- Ethernet (não bridge 802.1d)
- Ethernet Wireless (802.11)

Segmentos compartilhados L2 ponto-multiponto

- Ethernet (não bridge 802.1d)
- Ethernet Wireless (802.11)

Atenção muito cuidado em conferências !



TSIG

Transaction Signatures – RFC 2845

- Tráfego assinado com uma chave compartilhada (simétrica) entre as duas partes
- Utilizado principalmente em transferências de zona (master e slave)

TSIG

Transaction Signatures — RFC 2845

- Tráfego assinado com uma chave compartilhada (simétrica) entre as duas partes
- Utilizado principalmente em transferências de zona (master e slave)

DNSSEC

- Assinatura digital das informações da zona
- Utiliza o conceito de chaves assimétricas (pública e privada)
- Garante integridade e autenticidade das informações
- Provê segurança para a resolução de endereços

Parte II

DNSSEC



Domain Name System **SEC**urity extensions

- Extensão da tecnologia DNS
(o que existia continua a funcionar)
- Possibilita maior segurança para o usuário na Internet
(corrige algumas vulnerabilidades do DNS)
- Atualmente na versão denominada DNSSEC bis com opcional NSEC3

O que garante?

- Origem (Autenticidade)
- Integridade
- A não existência de um nome ou tipo

O que garante?

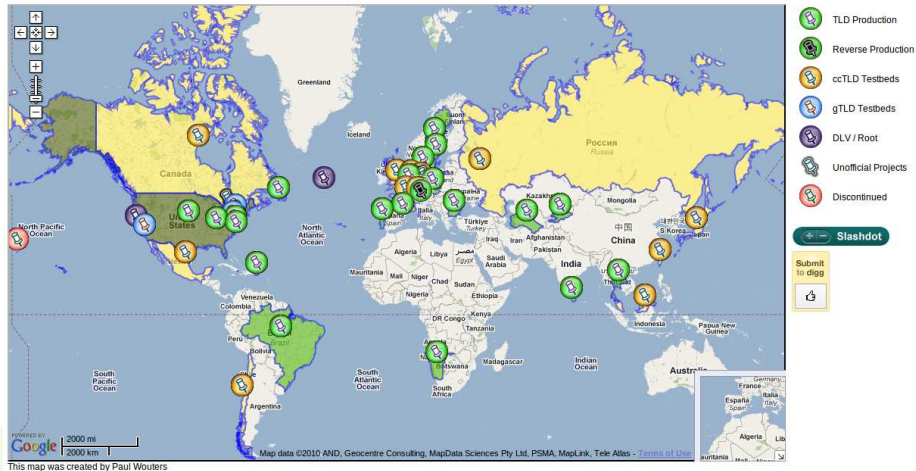
- Origem (Autenticidade)
- Integridade
- A não existência de um nome ou tipo

O que NÃO garante?

- Confidencialidade
- Proteção contra ataques de negação de serviço (DOS)

World Wide DNSSEC Deployment

See also [DNSSEC Theory and World Wide Deployment](#) by Paul Wouters, November 21, 2007, [SecTor](#)



Quem pode utilizar DNSSEC abaixo do .br?

Todos os domínios abaixo do .br podem (e devem) utilizar DNSSEC.
Atualmente com cerca de 250.000 domínios assinados (9%)

Mais informações podem ser obtidas no site <http://www.registro.br/dominio/dpn.html>

Quem pode utilizar DNSSEC abaixo do .br?

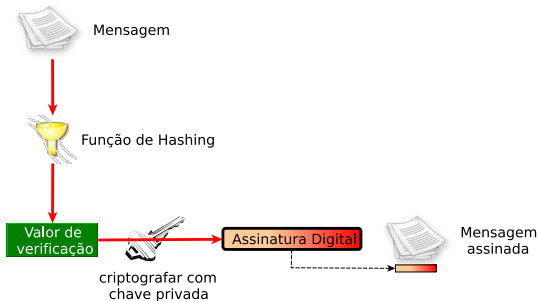
Todos os domínios abaixo do .br podem (e devem) utilizar DNSSEC. Atualmente com cerca de 250.000 domínios assinados (9%)

Mais informações podem ser obtidas no site <http://www.registro.br/dominio/dpn.html>

Onde DNSSEC é Obrigatório?

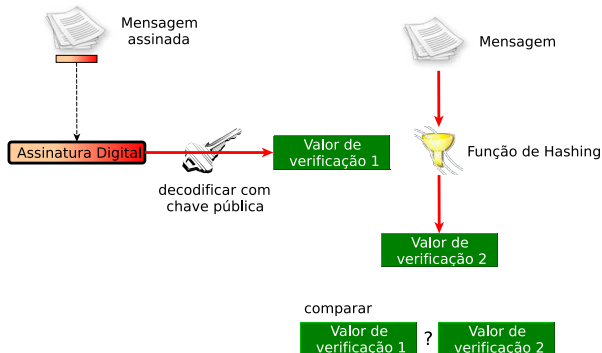
É obrigatório nos registros que estiverem diretamente abaixo dos domínios .B.BR e .JUS.BR

Assinatura



DNSSEC utiliza o conceito de chaves assimétricas
– chave pública e chave privada

Verificação



DNSSEC utiliza o conceito de chaves assimétricas
— chave pública e chave privada

- DNSKEY Chave pública (incluída na própria zona)
- RRSIG Assinatura do RRset (somente registros com autoridade)
- DS Delegation Signer (Ponteiro para a cadeia de confiança)
- NSEC(3) Next Secure (Prova de não existência)

Representa a chave pública de uma zona

```

                                1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|                               Flags                               |
+-----+-----+-----+-----+-----+-----+-----+-----+
/                                                                 /
/                               Public Key                          /
/                                                                 /
+-----+-----+-----+-----+-----+-----+-----+-----+
```

```
$ dig foo.eng.br dnskey +dnssec
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26230  
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
```

```
;; OPT PSEUDOSECTION:
```

```
; EDNS: version: 0, flags: do; udp: 1280
```

```
;; QUESTION SECTION:
```

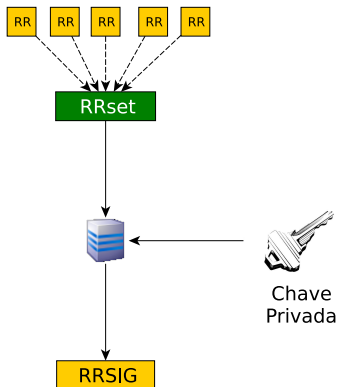
```
;foo.eng.br. IN DNSKEY
```

```
;; ANSWER SECTION:
```

```
foo.eng.br. 70946 IN DNSKEY 257 3 5 (  
    AwEAAa1ZWwcbEa05xKyJVyIC1inc/DclqTWIhlUsYiuy  
    qbiC7Kz5lw0YMPNh00edsC3d9S6Ccjo6T30UMjFfA+FS  
    wf7eqtv09w7XeuAg9uNdS6wtDL6Qz+UTv9qUzpdclaHK  
    TY8VIfy1Kc8XkR2lgbnfFZkhKlactVJMD4dsUUUJIryF  
    ) ; key id = 58729
```

```
foo.eng.br. 70946 IN RRSIG DNSKEY 5 3 86400 20120516101147 (  
    20120426101147 58729 foo.eng.br.  
    LFT+hSwL6MeFxB2021iuLocmmR8ua6BmphAan7FXCero  
    SwvEKwvFLLo5piyDkBY5opSLWhbRInahw3F/SZqxt+I  
    MY/zleKOY646+ZvRP4Jt4wjnx2kJG2Bp1NddiFSPoK4X  
    17+DRgB0s80M9kzfEw10FSEJH2HQ/v+g3zgN770= )
```

- Representa a assinatura de um RRset específico com uma determinada chave (DNSKEY)
- Possui uma validade inicial (inception) e final (expiration)



Exemplos de RRset:

```
foo.eng.br.      IN NS ns1.foo.eng.br.  
foo.eng.br.      IN NS ns2.foo.eng.br.
```

```
ns1.foo.eng.br.  IN A 200.160.3.97
```

```
ns2.foo.eng.br.  IN A 200.160.3.97
```

```

                                1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|          Type Covered          | Algorithm | Labels |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                Original TTL                                |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                Signature Expiration                        |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                Signature Inception                        |
+-----+-----+-----+-----+-----+-----+-----+-----+
|          Key Tag          |                               Signer's Name      /
+-----+-----+-----+-----+-----+-----+-----+-----+
/                               /
+-----+-----+-----+-----+-----+-----+-----+-----+
/                               /
/                               /
/                               /
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                Signature                                |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

```
$ dig @200.160.10.251 foo.eng.br SOA +dnssec +noadditional
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 6372
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 5
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;foo.eng.br.          IN      SOA
;; ANSWER SECTION:
foo.eng.br.  900    IN      SOA      ns1.foo.eng.br. hostmaster.foo.eng.br. 1 3600 3600 3600 900
foo.eng.br.  900    IN      RRSIG     SOA 5 3 900 20070617200428 20070518200428 62745 foo.eng.br.
           glEeCYyd/CCBfzh64y0RAQf90xYDsI4xuBNaam+8DZQZxeoSLQEEtwp
           6wBtQ7G10wSM9nEjRRhbZdNPNKJMp2PElLLgLI+BLwdlz0t8MypcpL0a
           Tm9rc7pP7UR5XLzU1k8Dm6ePW1bNkId7i0IPSghyoHM7tPVdL2GW51hCuJA=

;; AUTHORITY SECTION:
foo.eng.br.  900    IN      NS       ns2.foo.eng.br.
foo.eng.br.  900    IN      NS       ns1.foo.eng.br.
foo.eng.br.  900    IN      RRSIG     NS 5 3 900 20070617200428 20070518200428 62745 foo.eng.br.
           3iLm1ROC+UeqYk0xgQGQXkBzcKiKQRPwe+1JZlpjEzjU1UjOHUOHefa
           jXzMv7F1FMWYeU51Ybg49HFe67XQVlK54GeAFXWB7YS59yODLoNEBxQ1
           9QEY6g/00nLpuKTrST8qqd5Fc/eYqN/Ag3GnfcAviZgiQhhveGH9mJHWZyc=
```

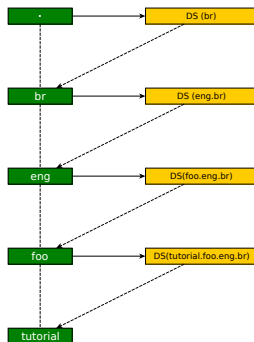
Representa um hash de um record DNSKEY

Indica:

- que a zona delegada está assinada
- qual a chave usada na zona delegada

A zona Pai possui autoridade pelo record DS das zonas delegadas

- O record DS **não** deve aparecer no Filho



Cadeia de Confiança

O Record DS forma uma cadeia de confiança, a qual garante a autenticidade das delegações de uma zona até um ponto de confiança (uma chave ancorada)

```

                                1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 3 3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|           Key Tag           | Algorithm | Digest Type |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
/                               /
/                               /
/                               /
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

Exemplo

foo.eng.br.

IN DS 817 5 1 EAEC29E4B0958D4D3DFD90CC70C6730AD5880DD3

É possível obter os DS da zona utilizando o sistema Whois.

Exemplo de DS pelo Whois

\$ whois foo.eng.br

```
domain:      foo.eng.br
owner:       Frederico A. C. Neves
address:     Av. das Nacoes Unidas, 11541, 7 andar
address:     04578-000 - São Paulo - SP
country:     BR
owner-c:     FAN
admin-c:     FAN
tech-c:      FAN
billing-c:   FAN
nserver:     dixit.foo.eng.br 200.160.7.134
nsstat:      20070619 AA
nslastaa:    20070619
nserver:     sroot.dns.br
nsstat:      20070619 AA
nslastaa:    20070619
ds-record:   6928 RSA/SHA-1 CA7D9EE79CC37D8DC8011F33D330436DF76220D1
created:     20000103 #237812
expires:     20080103
changed:     20070604
status:      published
```

- Indica o próximo nome seguro na zona
- Indica os tipos de RRsets existentes para o nome
- Circular (Último aponta para o primeiro)

```

      1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
/                               Next Domain Name                               /
+-----+-----+-----+-----+-----+-----+-----+-----+
/                               Type Bit Maps                               /
+-----+-----+-----+-----+-----+-----+-----+-----+

```

foo.eng.br.

```
900 IN NSEC ns1.exemplo.foo.eng.br. NS SOA RRSIG NSEC DNSKEY
```

60 / 119

● Respostas **NXDOMAIN**

- Um ou mais registros NSEC indicam que o nome ou a sintetização de um wildcard não existe

```
$ dig @200.160.10.251 zzz.foo.eng.br SOA +dnssec
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 18301
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1
;; QUESTION SECTION:
;zzz.foo.eng.br.      IN      SOA
;; AUTHORITY SECTION:
foo.eng.br.          0       IN      SOA      ns1.foo.eng.br. hostmaster.foo.eng.br. 1 3600 3600 3600 900
foo.eng.br.          0       IN      RRSIG     SOA 5 3 900 20070617200428 20070518200428 62745 foo.eng.br.
                        glEeCYyd/CCBfzH64yORAQf90xYDsI4xuBNaam+8DZQZxeoSLQEetwmp
                        6wBtQ7G10wSM9nEjRRhbZdNPNKJMp2PEllLgLI+BLwdlz0t8MypcpL0a
                        Tm9rc7pP7UR5XLzU1k8Dm6ePW1bNkId7i0IPSghyoHM7tPVdL2GW51hCuJA=
foo.eng.br.          900     IN      NSEC      ns1.exemplo.foo.eng.br. NS SOA RRSIG NSEC DNSKEY
foo.eng.br.          900     IN      RRSIG     NSEC 5 3 900 20070617200428 20070518200428 62745 foo.eng.br.
                        OCOcPFW5fR6MPHVBaUWfrP9pkIqVc+NDORi6PRwIX/pidLmAT7NF5Rkc
                        9IfbAHZTxfefoqTKqN/vPl1PqSxUzh0rl+atHb1ah6yt79CTkmStota7C
                        SLYYX5c7D93hRYJ2yk1C0xQz6GG9SIp/U4qR4//TcQDHPqQ4bFs42ZsD4I=
ns2.foo.eng.br.      900     IN      NSEC      foo.eng.br. A RRSIG NSEC
ns2.foo.eng.br.      900     IN      RRSIG     NSEC 5 4 900 20070617200428 20070518200428 62745 foo.eng.br.
                        XVf7M09L4rVUD6uxa1P+EhQYohuimuwk1xzAemsn292esUhhkYz/BG7b
                        OT/L9fhz0EYPtYGFyMF4gZ1/mxwY31UmX6xVZZPYFJ7x5Kw2uTSD49FK
                        VsdUOLBCAHZ088byAm8EwLe31+U0/q8RvPimAfpuouivUDcuWtKxs0CzLyc=
```

- Resposta **NOERROR** + sem resposta (ANSWER = 0)
 - O registro NSEC prova que o tipo consultado não existe

```
$ dig @200.160.10.251 foo.eng.br TXT +dnssec
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60466
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1
;; QUESTION SECTION:
;foo.eng.br.                IN      TXT
;; AUTHORITY SECTION:
foo.eng.br.  900  IN      SOA      ns1.foo.eng.br. hostmaster.foo.eng.br. 1 3600 3600 3600 900
foo.eng.br.  900  IN      RRSIG    SOA 5 3 900 20070617200428 20070518200428 62745 foo.eng.br.
              glEeCYyd/CCBfzH64yORAQf90xYDsI4xuBNaam+8DZQZxeoSLQEetwmp
              6wBtQ7G10wSM9nEjRRhbZdNPNKJMp2PELLgLI+BLwdlz0t8MypcpL0a
              Tm9rc7pP7UR5XLzU1k8Dm6ePW1bNkId7i0IPSghyoHM7tPVdL2GW51hCuJA=
foo.eng.br.  900  IN      NSEC    ns1.exemplo.foo.eng.br. NS SOA RRSIG NSEC DNSKEY
foo.eng.br.  900  IN      RRSIG    NSEC 5 3 900 20070617200428 20070518200428 62745 foo.eng.br.
              OCOCpFw5fR6MPHVBaUwfrP9pkIqVc+NDORi6PRwIX/pidLmAT7NF5Rkc
              9IfbAHZTxefoqTKqN/vP11PqSxUzh0rl+atHb1ah6yt79CTkmStota7C
              SLYYXX5c7D93hRYJ2yk1C0xQz6GG9SIP/U4qR4//TcQDHpqQ4bFs42ZsD4I=
```

- RFC 5155
- Soluciona o problema do “Zone Walking”
- Substitui o record NSEC pelo record NSEC3
- Consiste na sequência de hashes dos nomes da zona
- COM.BR e NET.BR

- RRsets são assinados com a chave privada da zona, gerando RRSIGs
- Chave pública é usada para verificar a assinatura (RRSIG) dos RRsets
- Autenticidade da chave é verificada pelo record DS assinado na zona pai (hash da chave pública da zona filha)
- NSEC fornece prova de não existência

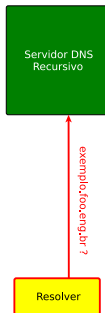
- Não existem Certificados
(Certification Authority, Service Level Agreement, Certificate Revocation List)
- Chaves nunca expiram
- Assinaturas têm prazo de validade
(inception e expiration do RRSIG)
- Políticas das chaves são locais à zona

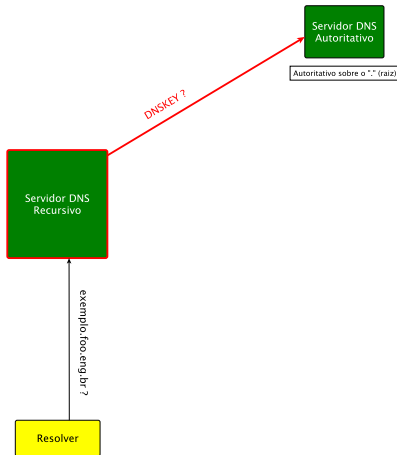
Para habilitar um servidor recursivo com DNSSEC é necessário ancorar uma chave pública, que servirá como início da cadeia de confiança.

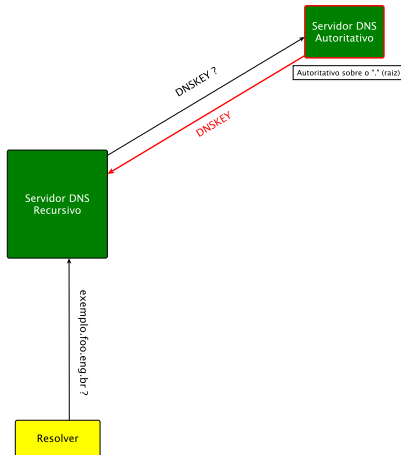
Obtendo a chave da zona “.” (raiz)

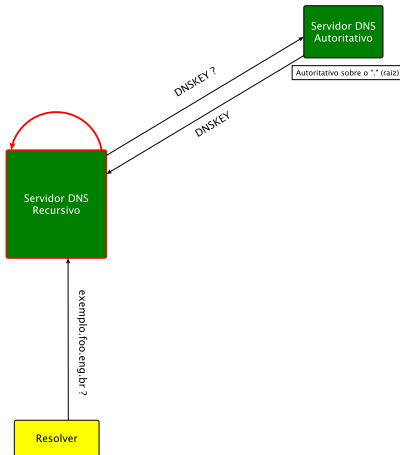
- <https://registro.br/ dominio/root-anchor.html>

- O resolver recursivo já possui a chave pública da zona “.” (raiz) ancorada

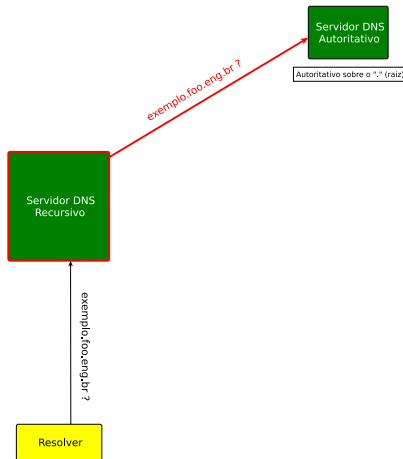


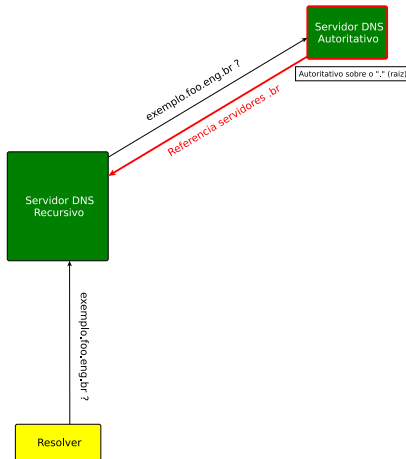




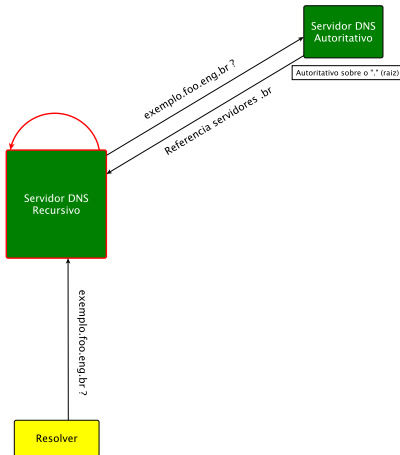


- Compara a chave ancorada com a DNSKEY, caso seja válida continua com as requisições

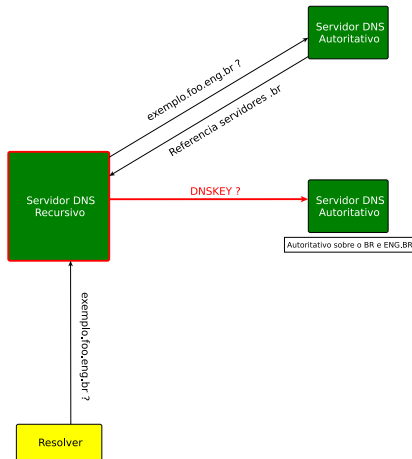




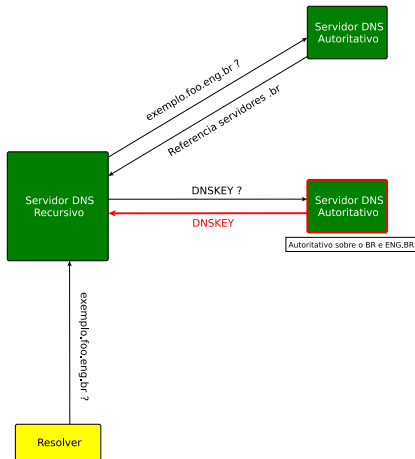
- Retorna sem resposta, mas com referência para “br”:
 - NS de “br”
 - DS de “br”
 - RRSIG do Record DS

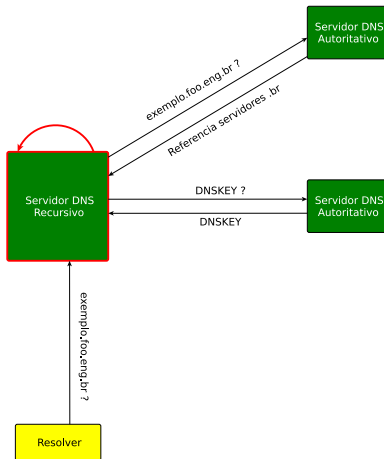


- O servidor DNS recursivo utiliza a DNSKEY para checar a assinatura (RRSIG) do Record DS

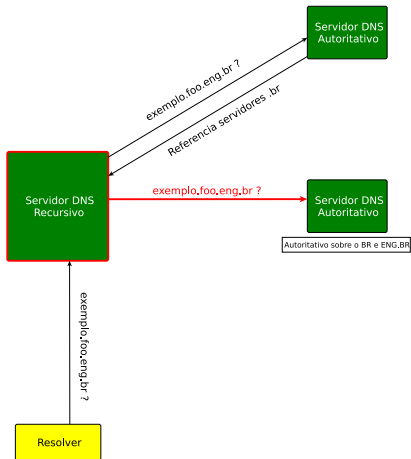


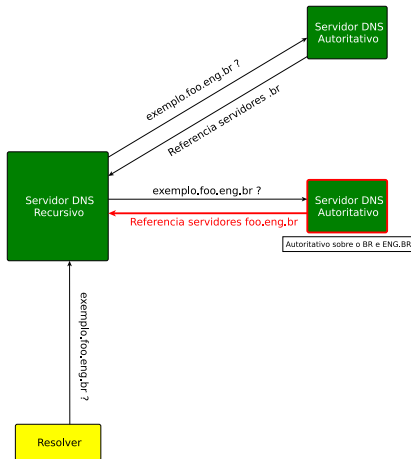
- O servidor DNS responde enviando DNSKEY e o RRSIG





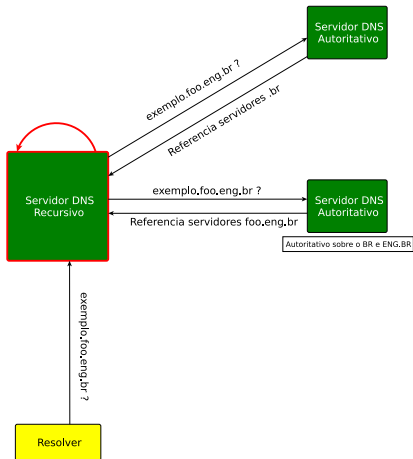
- O servidor DNS recursivo verifica, através do DS, se a DNSKEY é válida.

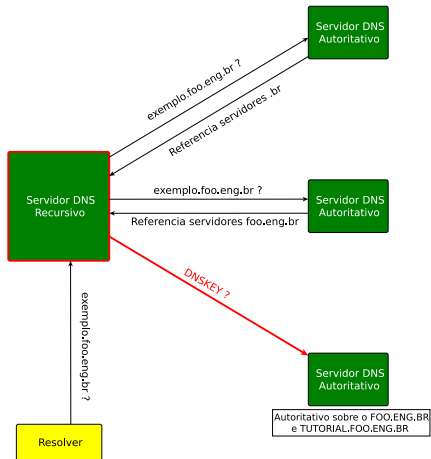


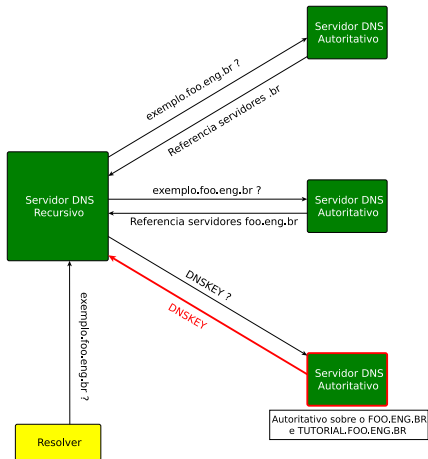


- Retorna sem resposta, mas com referência "foo.eng.br":
 - NS de "foo.eng.br"
 - DS de "foo.eng.br"
 - RRSIG do Record DS

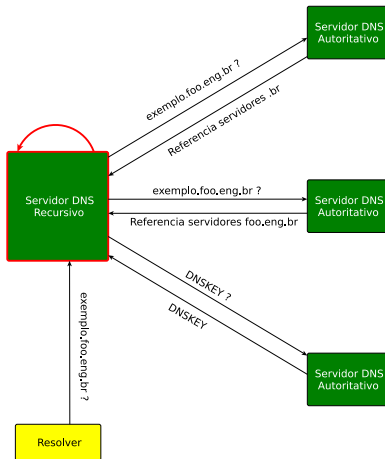
- O servidor DNS recursivo utiliza a DNSKEY para checar a assinatura (RRSIG) do Record DS

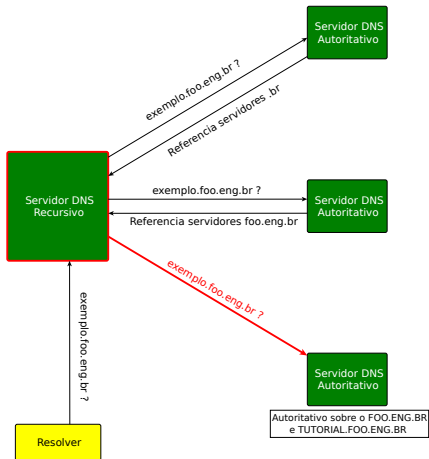




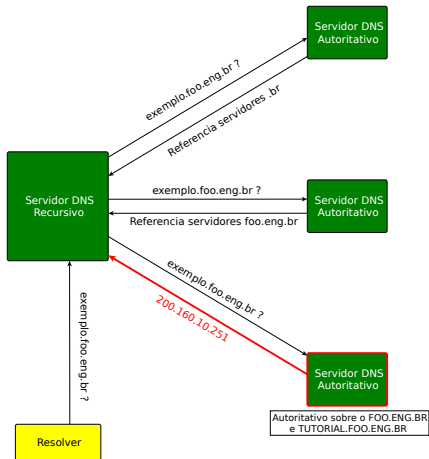


- O servidor DNS recursivo verifica, através do DS, se a DNSKEY é válida.

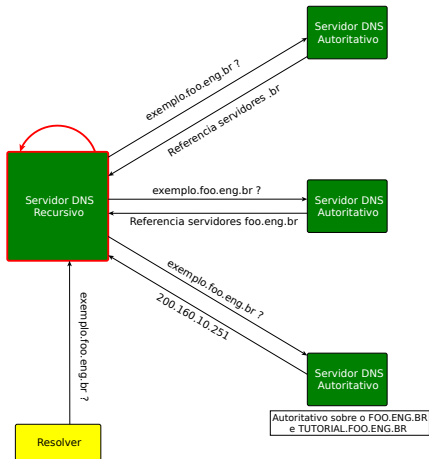


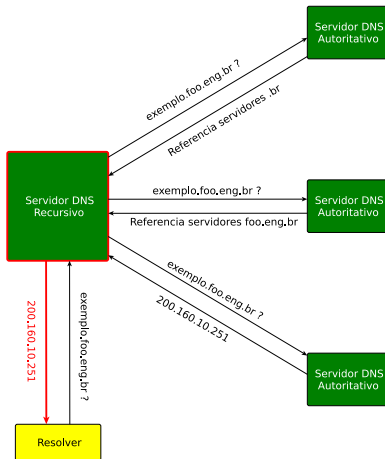


- Retorna o Record A e sua assinatura RRSIG.



- O servidor DNS recursivo utiliza a DNSKEY para checar a assinatura (RRSIG) do Record A





- Outra extensão ao protocolo DNS
- Distingue quem suporta DNSSEC
- Possibilita mensagens DNS UDP maiores que 512 bytes
 - ▶ Mensagens DNSSEC são bem maiores

Lembrete

É necessário que o transporte TCP também esteja habilitado no servidor.

Configuração de Firewall

O firewall deve ser capaz de tratar corretamente fragmentos UDP.



Configuração de Firewall

O firewall deve ser capaz de tratar corretamente fragmentos UDP.

Caso isto não seja possível, uma alternativa é configurar o servidor para trabalhar com pacotes UDP menores que o MTU da rede.

```
options {  
    edns-udp-size 1252; # Servidores recursivos  
    max-udp-size 1252; # Servidores recursivos e autoritativos  
};
```

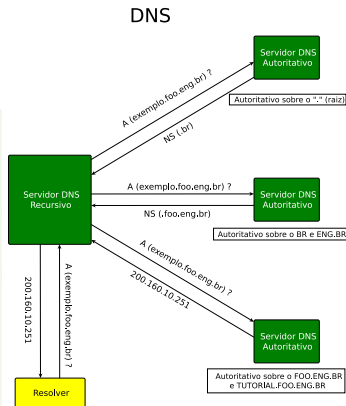
1252 é apenas uma sugestão, este valor deve refletir as configurações de Firewall.

Recomendação

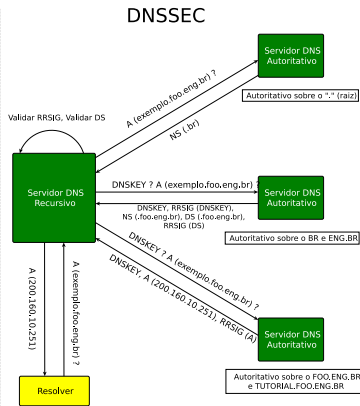
Firewalls e DNS, como e porque configurar corretamente

<ftp://ftp.registro.br/pub/doc/dns-fw.pdf>

Diferenças entre uma requisição DNS e uma requisição DNSSEC:



8 Pacotes — X Bytes



12 Pacotes ± 6X Bytes^a

^aDiferença proporcional ao tamanho da chave

	Autoritativo	Recursivo	DNSSEC bis ^a	NSEC3 ^b	RFC 5011	TSIG	IPv6
ANS	✓		✓			✓	✓
BIND	✓	✓	✓	✓ ^c	✓	✓	✓
djbdns	✓	✓					✓
DNSSHIM	✓		✓			✓	✓
IPControl	✓	✓	✓			✓	✓
IPM DNS	✓	✓	✓			✓	✓
MaraDNS	✓	✓					
Microsoft DNS	✓	✓	✓ ^d			✓	✓
NSD	✓		✓	✓	✓	✓	✓
PowerDNS	✓	✓					✓
Unbound		✓	✓	✓	✓		✓
Vantio		✓	✓			✓	✓
VitalQIP	✓	✓	✓				✓

^aVersão atual do protocolo

^bServidores recursivos devem(!) ter suporte a NSEC3 para pleno funcionamento com DNSSEC

^cSuporte a partir da versão 9.6.0

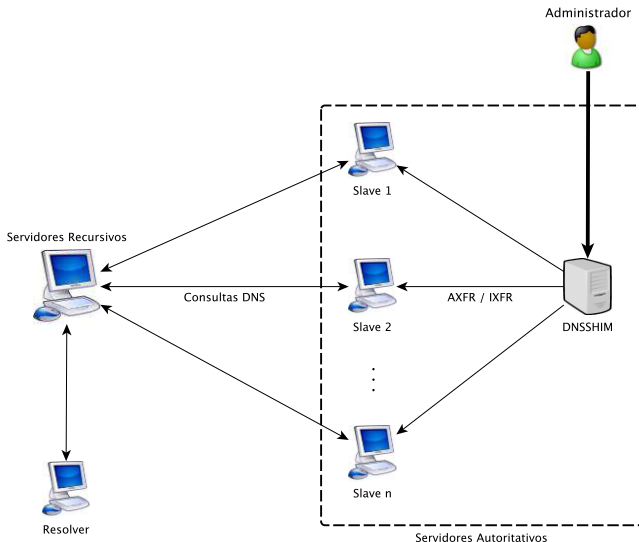
^dSuporte a partir da versão Windows Server 2008 R2 ou Windows 7

<http://registro.br/dnsshim/>

- Open-Source
- Automatiza o processo de provisionamento de zonas
- Suporte a DNSSEC
- Interface Automatizável
- Manutenção de chaves/assinaturas

Público Alvo

Provedores de hospedagem ou qualquer outra instituição responsável por administrar servidores DNS autoritativos para **muitas zonas**



Parte III

Utilizando DNSSEC na Prática



DNSSEC no Servidor Autoritativo

Utilização do comando `dnssec-keygen` para geração de chaves:

```
$ dnssec-keygen -r /dev/urandom -f KSK dominio.com.br
```

Onde, **dominio.com.br** deve ser substituído pelo seu domínio.

- O comando irá gerar dois arquivos com extensões `.key` e `.private`

Mais informações no Apêndice III

Lembrete

Não se esquecer de incrementar o serial do SOA da zona!

Utilização do comando `dnssec-signzone` para assinatura

```
$ dnssec-signzone -S -z -o dominio.com.br db.dominio.com.br
```

Onde, **dominio.com.br** deve ser substituído pelo nome do domínio e **db.dominio.com.br** pelo nome do arquivo de zona.

- O comando irá gerar um novo arquivo de zona com a extensão `.signed`
- O período de validade padrão da assinatura é de 30 dias

Mais informações no Apêndice IV

Alteração da referência para o arquivo de zona

```
zone "dominio.com.br" {  
    type master;  
    file "/etc/namedb/db.dominio.com.br.signed";  
    ...  
};
```

Onde, **dominio.com.br** deve ser substituído pelo nome do domínio e **db.dominio.com.br** deve ser substituído pelo nome do arquivo de zona.



Reiniciar o Bind

Copiar os dados de **KeyTag** e **Digest** do arquivo **dsset-dominio.com.br** para a interface no site do Registro.br.

Exemplo: `$ cat dsset-dominio.com.br | head -1`

		KeyTag			Digest
dominio.com.br	IN DS	15469	5	1	5EC0184678E0B7DC3AACFFA5D0EB9DBA1F3F6C37

- Onde, **dominio.com.br** deve ser substituído pelo nome do domínio

DNSSEC

Record

KeyTag

Digest

DS 1

DS 2

Aguardar nova publicação no site do Registro.br

- 1 Criar chave (dnssec-keygen) (slide 118)
- 2 Assinar a zona (dnssec-signzone) (slide 120)
- 3 Modificar o named.conf (slide 103)
- 4 Reiniciar o BIND (named) no servidores Master
- 5 Adicionar o DS no site do Registro.br (slide 105)
- 6 Aguardar nova publicação

Servidor Autoritativo

Reassinar a zona antes das assinaturas expirarem

- 1 Incrementar o serial (record SOA) do arquivo de zona original
- 2 Reassinar a zona utilizando o comando `dnssec-signzone`

DNSSEC no Servidor Recursivo

Obter a chave da raiz no formato do Bind

<https://registro.br/dominio/root-anchor.html>

named.conf

```
managed-keys {  
    . initial-key 257 3 8  
        "AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLQyQbSEW008gcCjF  
        FVQUTf6v58fLjWbD0YIOEzrAcQqBGCzh/RStIo08gONfnfL2MTJRkxoX  
        bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD  
        X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz  
        W5h0A2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGicGOYl70yQdXfZ57re1S  
        Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq  
        QxA+Uk1ihz0=";  
};  
...
```

Reiniciar o Bind



[RFC 2671](#)

Extension Mechanisms for DNS (EDNS0)



[RFC 2845](#)

Secret Key Transaction Authentication for DNS (TSIG)



[RFC 4033](#)

DNS Security Introduction and Requirements (DNSSEC-bis)



[RFC 4034](#)

Resource Records for the DNS Security Extensions (DNSSEC-bis)



[RFC 4035](#)

Protocol Modifications for the DNS Security Extensions (DNSSEC-bis)



[RFC 4431](#)

The DNSSEC Lookaside Validation (DLV) DNS Resource Record



[RFC 4470](#)

Minimally Covering NSEC Records and DNSSEC On-line Signing



[RFC 4641](#)

DNSSEC Operational Practices



[RFC 5155](#)

DNSSEC Hashed Authenticated Denial of Existence

- ▶ **DNSSEC.NET**
<http://www.dnssec.net>
- ▶ **DNSSHIM**
<http://www.registro.br/dnsshim>
- ▶ **Wikipédia - DNSSEC**
<http://pt.wikipedia.org/wiki/DNSSEC>
- ▶ **Wikipédia - Comparação entre softwares de servidores DNS**
http://en.wikipedia.org/wiki/Comparison_of_DNS_server_software
- ▶ **Firewalls e DNS, como e porque configurar corretamente**
<ftp://ftp.registro.br/pub/doc/dns-fw.pdf>
- ▶ **Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos**
<http://www.cert.br/docs/whitepapers/dns-recursivo-aberto>
- ▶ **FAQ - Registro.br (Perguntas Frequentes)**
<http://registro.br/suporte/faq>
- ▶ **A última versão do tutorial de DNSSEC pode ser encontrada em**
<ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf>
- ▶ **DNSSEC – Olaf Kolkman (RIPE NCC/NLnet Labs)**
http://www.nlnetlabs.nl/dnssec_howto

Perguntas?

Fim da Apresentação

Referências

Obrigado!

- Serial** O número de revisão do arquivo de zona. Esse número aumenta cada vez que um record é alterado na zona.
- Refresh** O tempo, em segundos, que um servidor DNS secundário espera antes de consultar sua origem da zona para tentar renová-la.
- Retry** O tempo, em segundos, que um servidor secundário espera antes de tentar novamente uma transferência de zona falha.
- Expire** O tempo, em segundos, antes que o servidor secundário pare de responder às consultas depois de transcorrido um intervalo de atualização no qual a zona não foi renovada ou atualizada.
- Minimum** O menor tempo de vida (TTL) da zona e o intervalo máximo para armazenar respostas negativas em cache.

O que é

Um alias para nomes alternativos

Funcionalidade

Mapeia um nome de domínio alternativo ou apelido no campo *proprietário* para um canônico especificado no campo *Nome Canônico*

Problemas

- Records MX, NS, CNAME, e SOA só devem se referir a um record A.
- RRs referindo-se a um CNAME podem ocasionar problemas de buscas e carga extra na rede.
- Recomenda-se utilizar um RR A ao invés de CNAME.

BIND: dnssec-keygen

Zona foo.eng.br:

```
dnssec-keygen -f KSK -a RSASHA1 -b 2048 -n ZONE foo.eng.br
```

Onde,

- -f : Define o tipo da chave
- -a : Algoritmo
- -b : Tamanho da chave (bits)
- -n : Especifica o tipo de dono da chave
- -r : Device de randomização

Em determinados ambientes, onde a geração de chaves demorar muito pode ser necessário especificar o device de randomização, como por exemplo: “-r /dev/urandom”

OBS1: Guardar o nome das chaves geradas para ser usado futuramente.

OBS2: Chaves geradas com dnssec-keygen não possuem passphrase.

Exemplo de Tamanho de chaves

- BR: 1280 bits

Chave pública (.key)

```
foo.eng.br. IN DNSKEY 257 3 5 AwEAAaDaICi4nCQX+dC+kkG1Gmi7+Pjww405WYZtt+oe1RG329H2+k0Y XhYiZx7tLULD8Fn3DtBC
hGTeFND+gCBjOvFS9MEjxHIkD2gtt3fFibqN /sQIHDjNGr1M6aFngKxWTENWqkl71ht9j0EvzsLOD+deFDge4sDF5q0Q 4D8njqI1IqDsU
kt3I1cJoFtP9k9RPIijxWdILWuKgh7nEvKpX7e0EuXO YK1W88Av9ctpm3y61zbsWCOK40I17nGTB+qMCbt/ZdYMWcaVuTBHQpEUKNVuq3m
FGj1MxwtadBimmq+YhleGzn21xOCYmsStwNUAWcb/H9SqOG F3CVcH0t86k=
```

Chave privada (.private)

```
Private-key-format: v1.2
Algorithm: 5 (RSASHA1)
Modulus: ONogKLicJBf50L6SQAuaLv4+PDDg71Zhm236h7VEbfb0fb6TRheFiJnHu0tQsPwWfc00EKEZN4UOP6AIGPS8VL0wSPEciQPac
23d8Uhuo3+xAgcOM0avUzpoWeArFZMQ1aqSXvWFP2M4S/Ows4P514UOB7iwMXmo5DgPyeOKogio0xSS3cjVwmgW0/2T1E8iKPFZ0gta4qCH
ucS8qlft44S5c5grVbzwC/1y2mbfLqXNuxYLRg4iXucZMH6owJu39l1gzBxpW5MEdCkRQo1W6reYUaPUzHC1pOGKaaqr5iGV4b0fbXHqJi
axK3A1QBZxv8f1KqDQYXcJVwfS3zqQ==
```

...

OBS

Antes de assinar a zona incrementalmente o serial do record SOA para que ocorra a sincronização com os servidores secundários.

Ao se assinar a zona são gerados os records RRSIG e NSEC que ficarão ordenados de forma canônica dentro do arquivo de zona.

BIND: dnssec-signzone

Zona foo.eng.br:

```
$ dnssec-signzone -S -z db.foo
```

Onde,

- -S : Assinatura inteligente - busca as chaves da zona e determina como estas utilizadas
- -z : Ignora o bit SEP da chave e assina toda a zona
- -e : Data de expiração das assinaturas (formato AAAAMMDDHHMMSS) - Se não informado é considerado 30 dias
- o último parâmetro se refere ao *arquivo de zona*

Geração de records DS

No momento em que se assina uma zona é gerado um arquivo contendo o Records DS que será utilizado para as delegações.

— o arquivo gerado neste exemplo: `dsset-foo.eng.br`.

Por que existem dois tipos de chave?

- Permite substituir uma chave de uso frequente (ZSK) sem ter a necessidade de modificar o DS do parent (hash da KSK)
- Permite criar uma chave de tamanho menor para criar assinaturas menores

Key Signing Key (KSK)

As chaves utilizadas para assinar as chaves da zona. Assinam apenas os RRsets do tipo DNSKEY — possui o flag **bit SEP** ligado

Zone Signing Key (ZSK)

As chaves utilizadas para assinar RRsets da zona sobre o qual tem autoridade

Lembrete

- O record DNSKEY pode armazenar tanto a chave pública de uma KSK quanto de uma ZSK
- O record RRSIG armazena a assinatura de um RRset realizada tanto por uma KSK quanto por uma ZSK

Lembrete

- O record DNSKEY pode armazenar tanto a chave pública de uma KSK quanto de uma ZSK
- O record RRSIG armazena a assinatura de um RRset realizada tanto por uma KSK quanto por uma ZSK

Trabalhando com uma única chave!

Entretanto é aconselhável a utilização de somente uma única chave. Mais informações sobre como proceder no slide 120.

Caso existam zonas delegadas que utilizem DNSSEC dentro do seu domínio, os Records DS destas zonas devem ser adicionados no arquivo de zona

Exemplo

```
SHA1 tutorial.foo.eng.br. IN DS 3112 5 1 386B4390C5B30DB65D74EA8B660978077171948C
```

```
SHA256 tutorial.foo.eng.br. IN DS 3112 5 2  
19602F6089F8877E037AA077B8376F30869E261EB55460F2A74E32AD1424F53A
```

```
foo.eng.br IN SOA ns1.foo.eng.br. hostmaster.foo.eng.br. (  
    3          ; serial  
    3600       ; refresh (1 hour)  
    3600       ; retry (1 hour)  
    3600       ; expire (1 hour)  
    900        ; minimum (15 minutes)  
)
```

```
foo.eng.br. IN NS ns1.foo.eng.br.
```

```
foo.eng.br. IN NS ns2.foo.eng.br.
```

```
...
```

```
tutorial.foo.eng.br. IN DS 3112 5 1 386B4390C5B30DB65D74EA8B660978077171948C
```

OBS

A zona deve ser re-assinada após incluir o record DS

BIND no Windows

- Faça o download da última versão do BIND em <http://www.isc.org>
- Descompacte o arquivo ZIP e execute o programa BINDInstall.exe
- Após a instalação, acesse os Serviços (ferramentas administrativas) e inicie o serviço “ISC BIND”

Erro ao iniciar o serviço ISC BIND

Acesse a propriedade do serviço, e na aba “Log On” selecione a opção “Local System account”

BIND no Windows

O BIND no Windows funciona da mesma forma que no Linux, sendo que os arquivos ficam localizados em locais diferentes.

- Os arquivos de configuração estão localizados em **c:\windows\system32\dns\etc**
- Os executáveis (named, dig) estão localizados em **c:\windows\system32\dns\bin**

The image displays three separate Command Prompt windows illustrating the setup and use of BIND on Windows.

- Top Left Window:** Shows the editing of `named.conf`. The configuration includes setting the `directory` to `"c:\windows\system32\dns\etc"`, enabling `dnssec-enable yes`, and setting `max-udp-size 8000`. A zone for `"foo.eng.br"` is defined with a master IP of `127.0.0.1` and a file `"c:\windows\system32\dns\etc\db.foo.signed"`.
- Top Right Window:** Shows the execution of `nslookup` for `foo.eng.br`. It displays the query details, including flags, question section, and the answer section showing the IP address `200.160.10.251`.
- Bottom Left Window:** Shows the execution of `dig` for `foo.eng.br`. It displays the query details, including flags, question section, and the answer section showing the IP address `200.160.10.251`.