Tutorial DNSSEC [1]

David Robert Camargo de Campos
Rafael Dantas Justo
<tutorial-dnssec@registro.br>

Registro.br

29 de Junho de 2007

[1] versão 1.3 (Revision: 3508)
A última versão deste tutorial pode ser encontrada em: ftp://ftp.registro.br/pub/doc/tutorial-DNSSEC.pdf

Objetivos

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

Cronograma

Parte I

Conceitos de DNS e DNSSEC

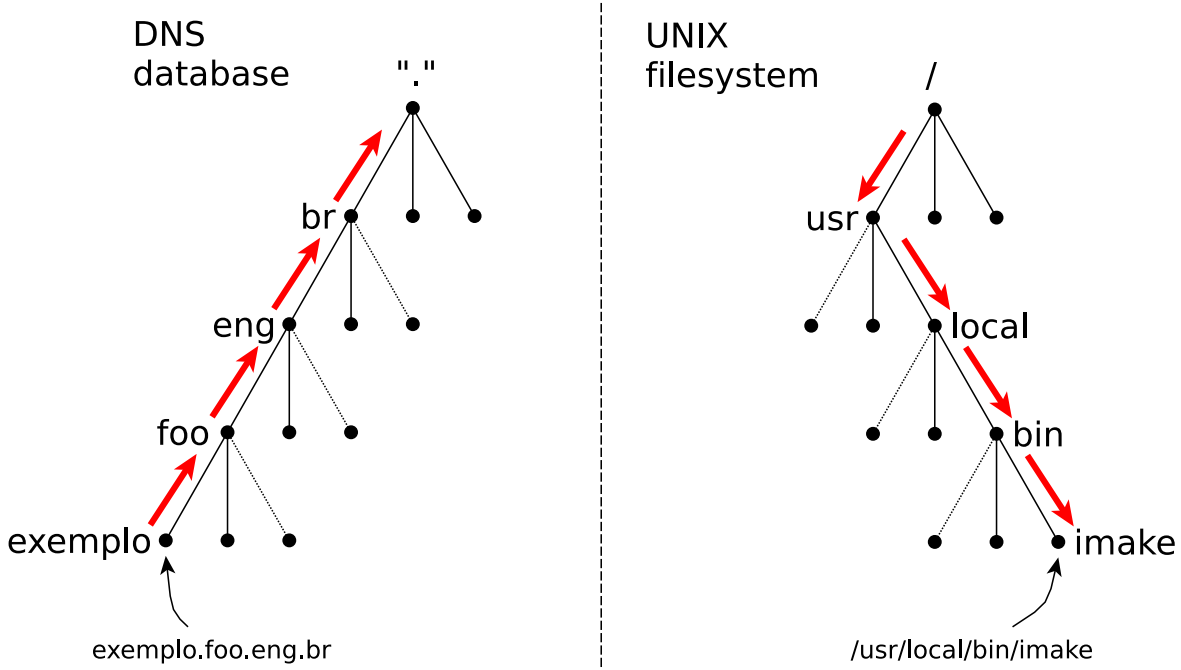
DNS - Domain Name System

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.

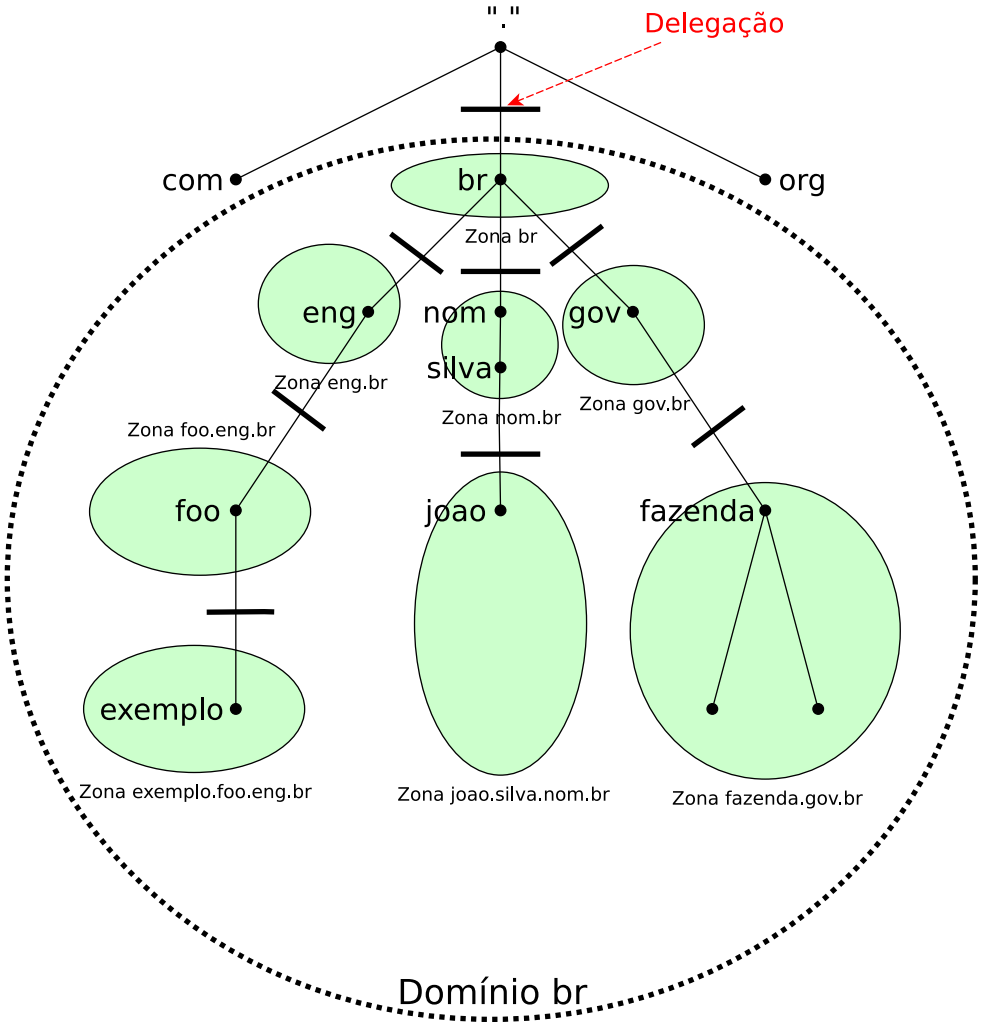
- Arquitetura hierárquica, dados dispostos em uma árvore invertida
- Distribuída eficientemente, sistema descentralizado e com cache
- O principal propósito é a resolução de nomes de domínio em endereços IP e vice-versa

exemplo.foo.eng.br	$\longleftrightarrow$	200.160.10.251
www.cgi.br	$\longleftrightarrow$	200.160.4.2

Hierarquia


DNS
database
"."
br
eng
foo
exemplo
exemplo.foo.eng.br
UNIX
filesystem
/
usr
local
bin
imake
/usr/local/bin/imake

Domínio Vs Zona



Delegação

Indica uma transferência de responsabilidade na administração apartir daquele ponto na árvore DNS

Registro de domínios (.br)

- Reserva o direito da pessoa física ou jurídica sobre um determinado nome de endereço na Internet.
- Domínios não registrados não podem ser encontrados na Internet.

Formas de registro

Sistema WEB

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

– http://registro.br/info/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/

Publicação quasi-on-line

registro.br
Registro de Domínios para a Internet no Brasil

O que é uma Publicação?

As modificações que são realizadas pela interface de provisionamento não são efetivadas imediatamente. A cada intervalo de tempo pré-determinado ocorre uma publicação DNS a qual atualiza o sistema DNS.

nic.br

Publicação quasi-on-line

registro.br
Registro de Domínios para a Internet no Brasil

O que é uma Publicação?

As modificações que são realizadas pela interface de provisionamento não são efetivadas imediatamente. A cada intervalo de tempo pré-determinado ocorre uma publicação DNS a qual atualiza o sistema DNS.

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).

Resource Records

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

- São divididos em classes e tipos
- Atualmente existe uma grande variedade de tipos
- O conjunto de resource records com o mesmo nome de domínio, classe e tipo é denominado **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

Exemplo de records de uma zona

```
foo.eng.br. IN SOA ns1.foo.eng.br. hostmaster.foo.eng.br. (
            1        ; serial
            3600     ; refresh
            3600     ; retry
            3600     ; expire
            900 )    ; minimum TTL
foo.eng.br.                IN NS ns1.foo.eng.br.
foo.eng.br.                IN NS ns2.foo.eng.br.
exemplo.foo.eng.br.        IN NS ns1.exemplo.foo.eng.br
exemplo.foo.eng.br.        IN NS ns2.exemplo.foo.eng.br
ns1.foo.eng.br.            IN A 200.160.3.97
ns2.foo.eng.br.            IN A 200.160.10.251
ns1.exemplo.foo.eng.br.  IN A 200.160.3.97
ns2.exemplo.foo.eng.br.  IN A 200.160.10.251
```

Tipos de servidores

registro.br
Registro de Domínios para a Internet no Brasil

Servidor Recursivo

Ao receber requisições de resolução de nomes, faz requisições para os servidores autoritativos e conforme a resposta recebida dos mesmos continua a realizar requisições para outros servidores autoritativos até obter a resposta satisfatória

Servidor Autoritativo

Ao receber requisições de resolução de nome, reponde um endereço caso possua, uma referência caso conheça o caminho da resolução ou uma negação caso não conheça

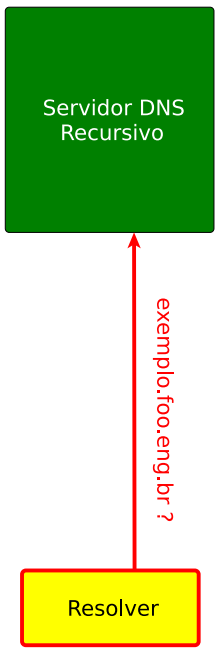
nic.br

Exemplo de requisição de endereço

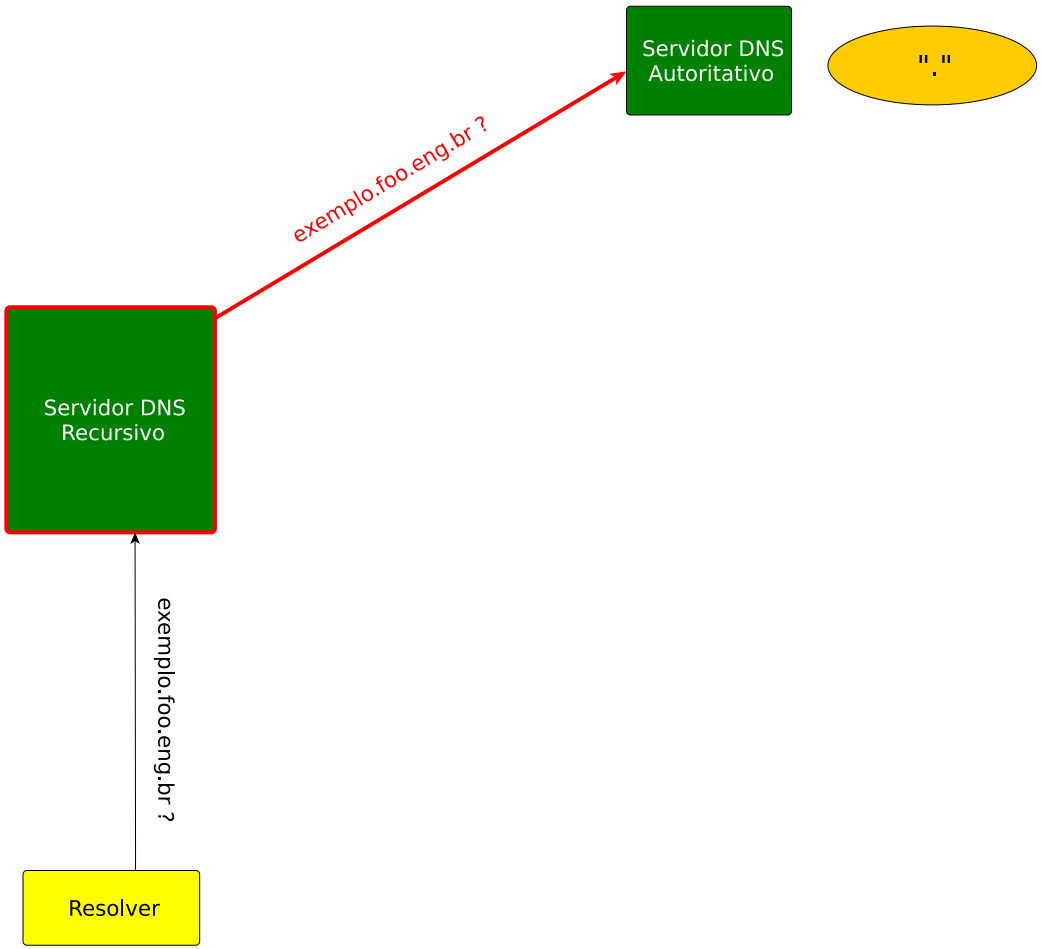
Supondo que o cache esta vazio ou sem informações de br, eng.br, foo.eng.br, exemplo.foo.eng.br

Resolver

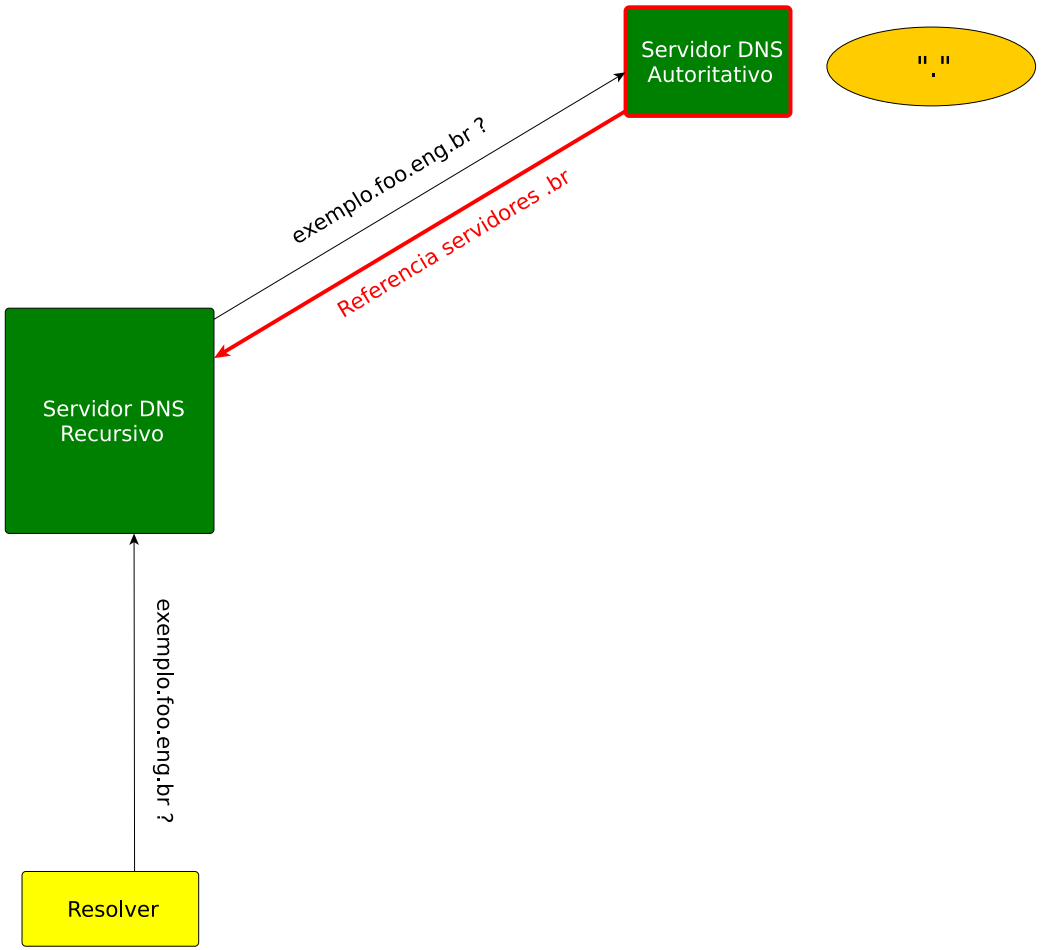
Exemplo de requisição de endereço



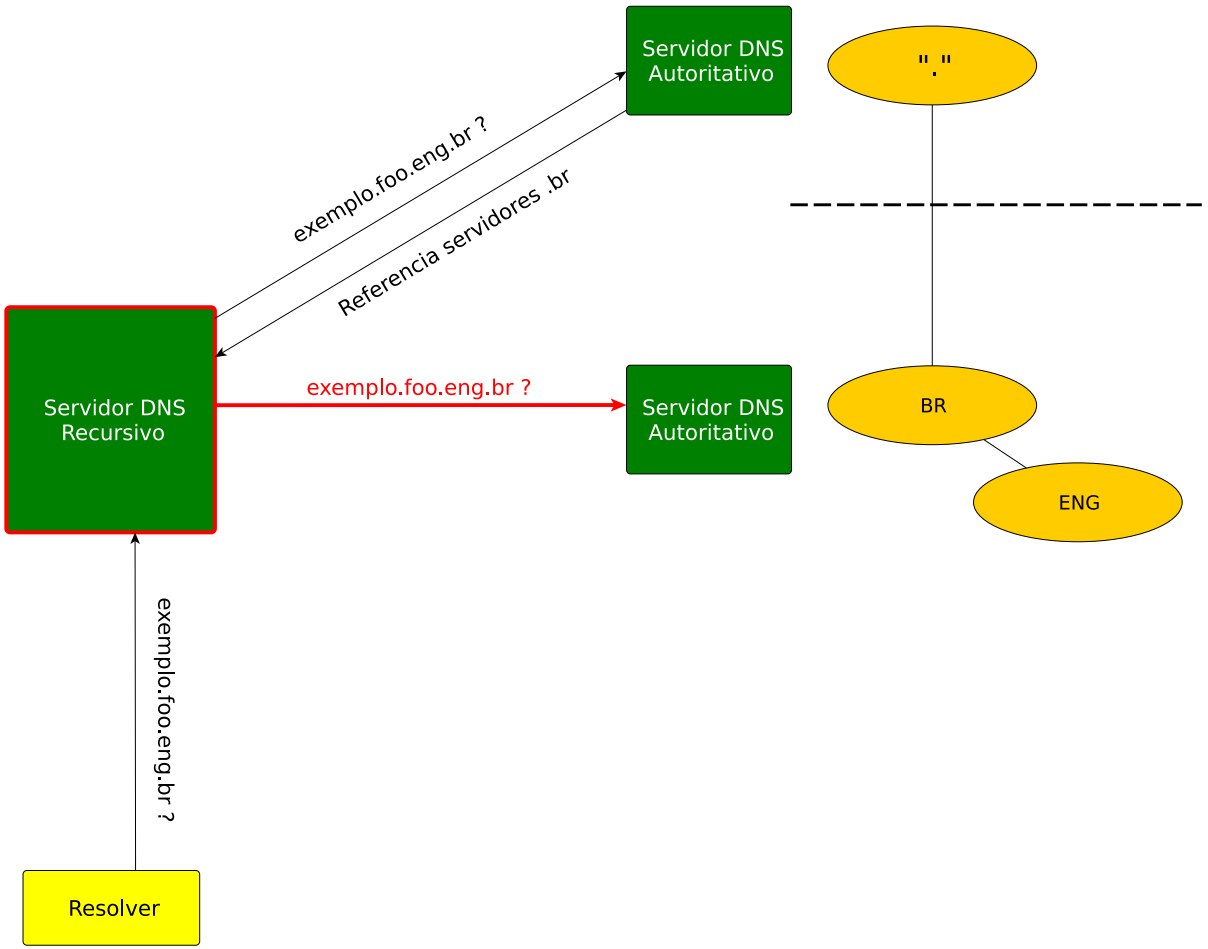
Exemplo de requisição de endereço



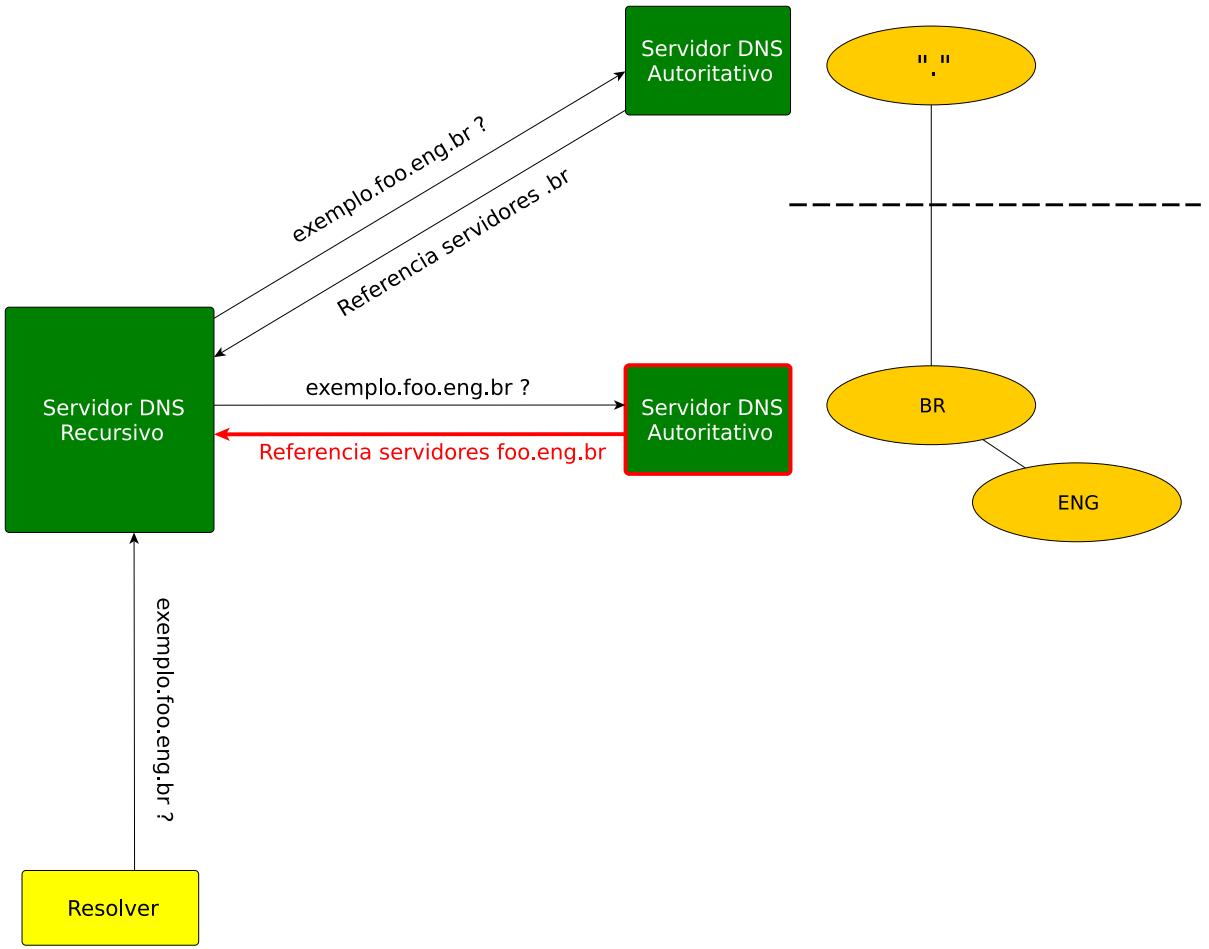
Exemplo de requisição de endereço



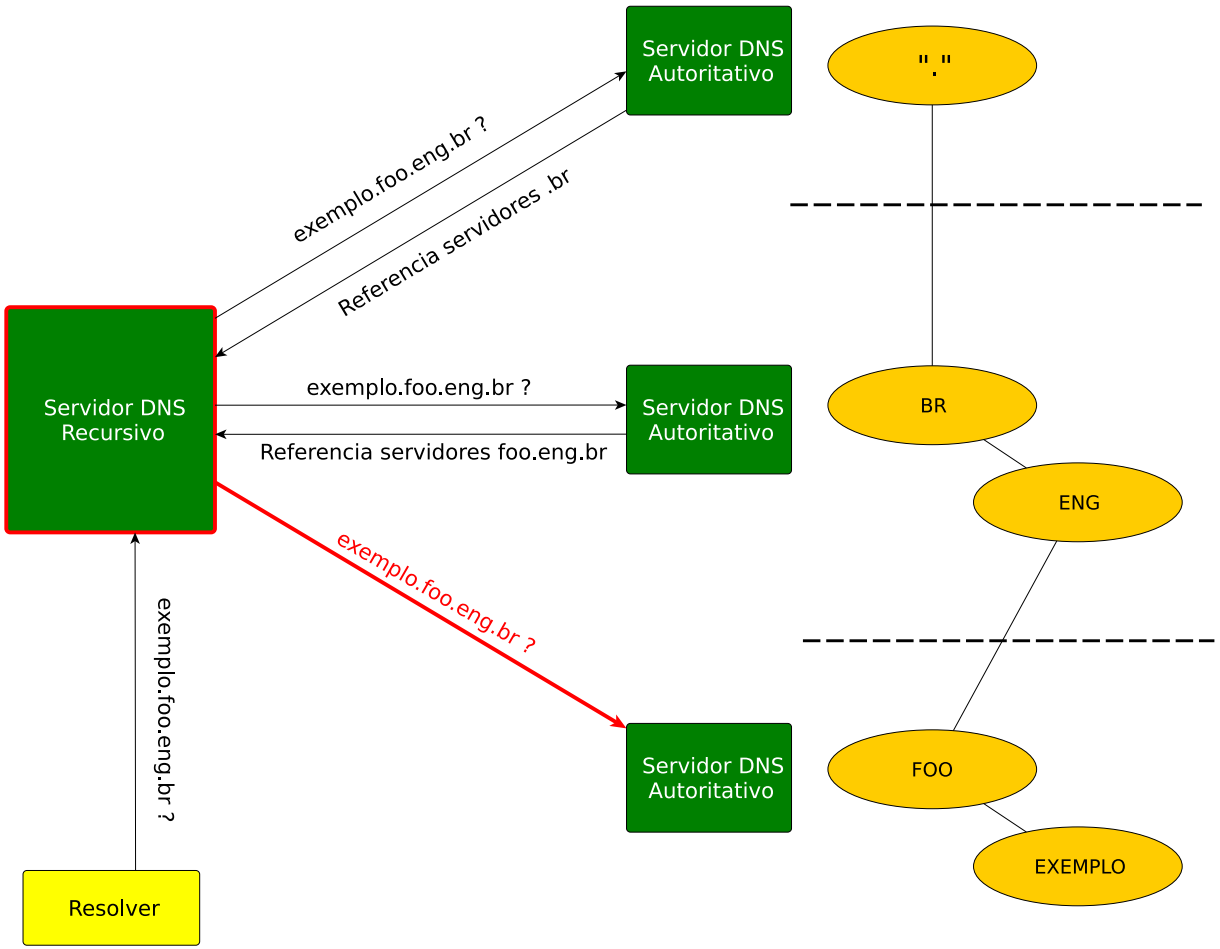
Exemplo de requisição de endereço



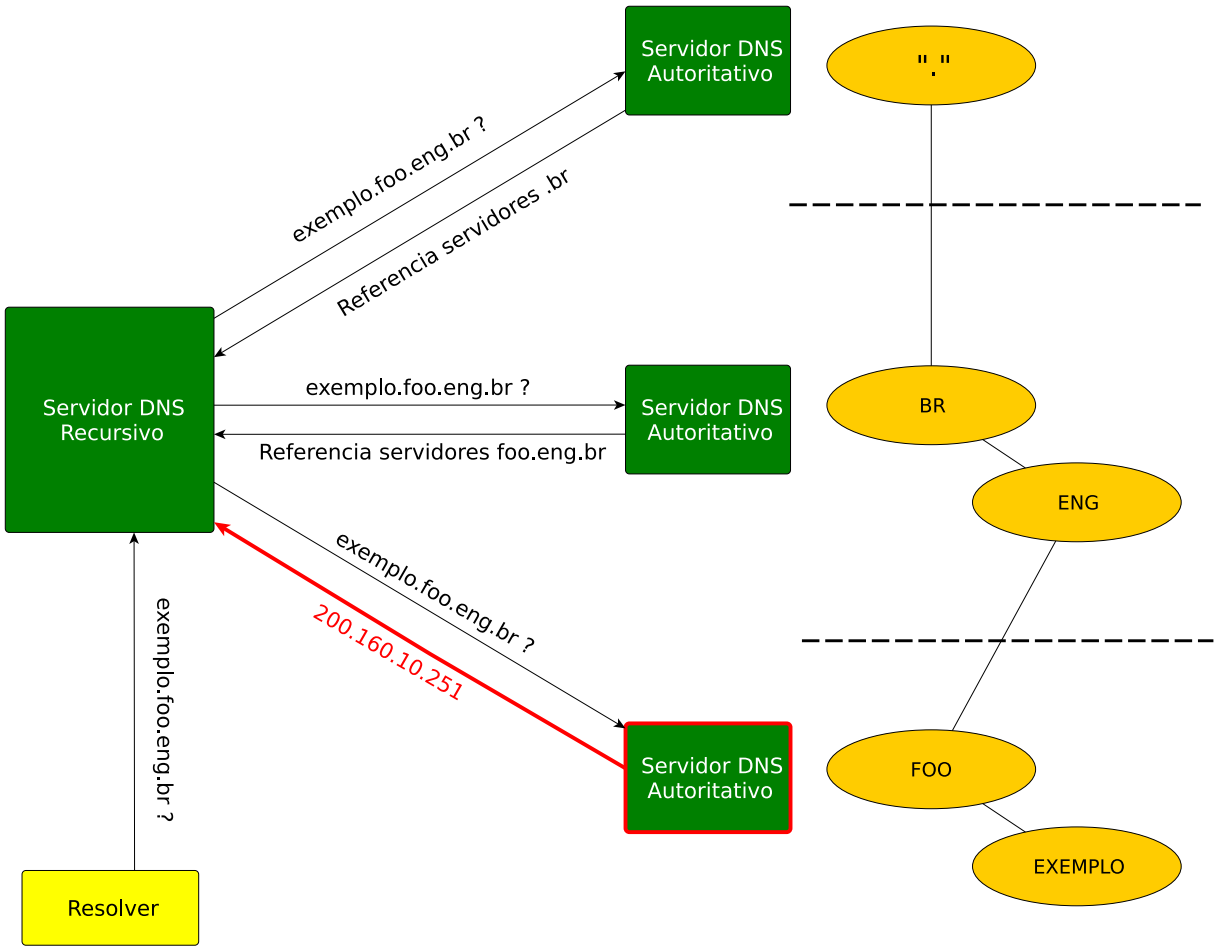
Exemplo de requisição de endereço



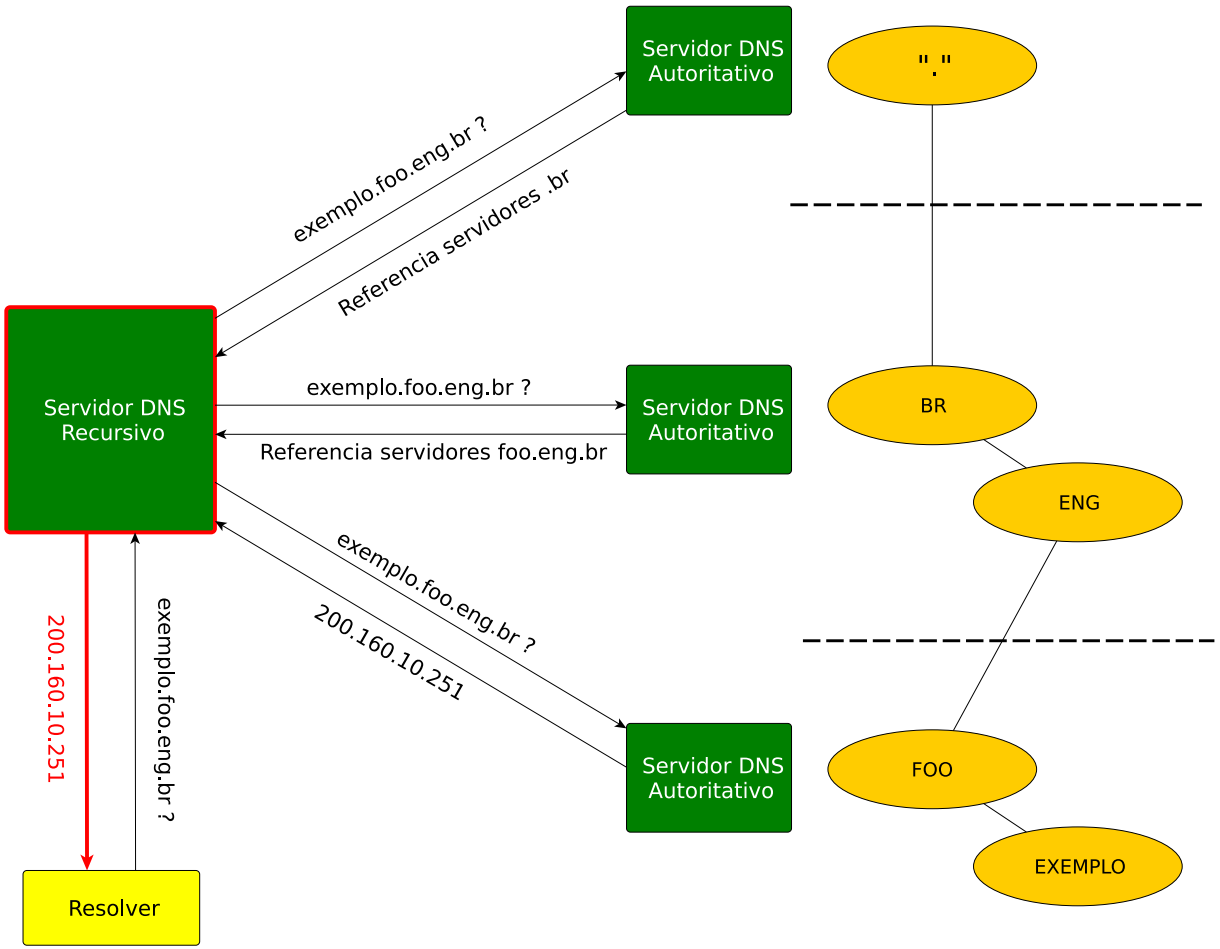
Exemplo de requisição de endereço



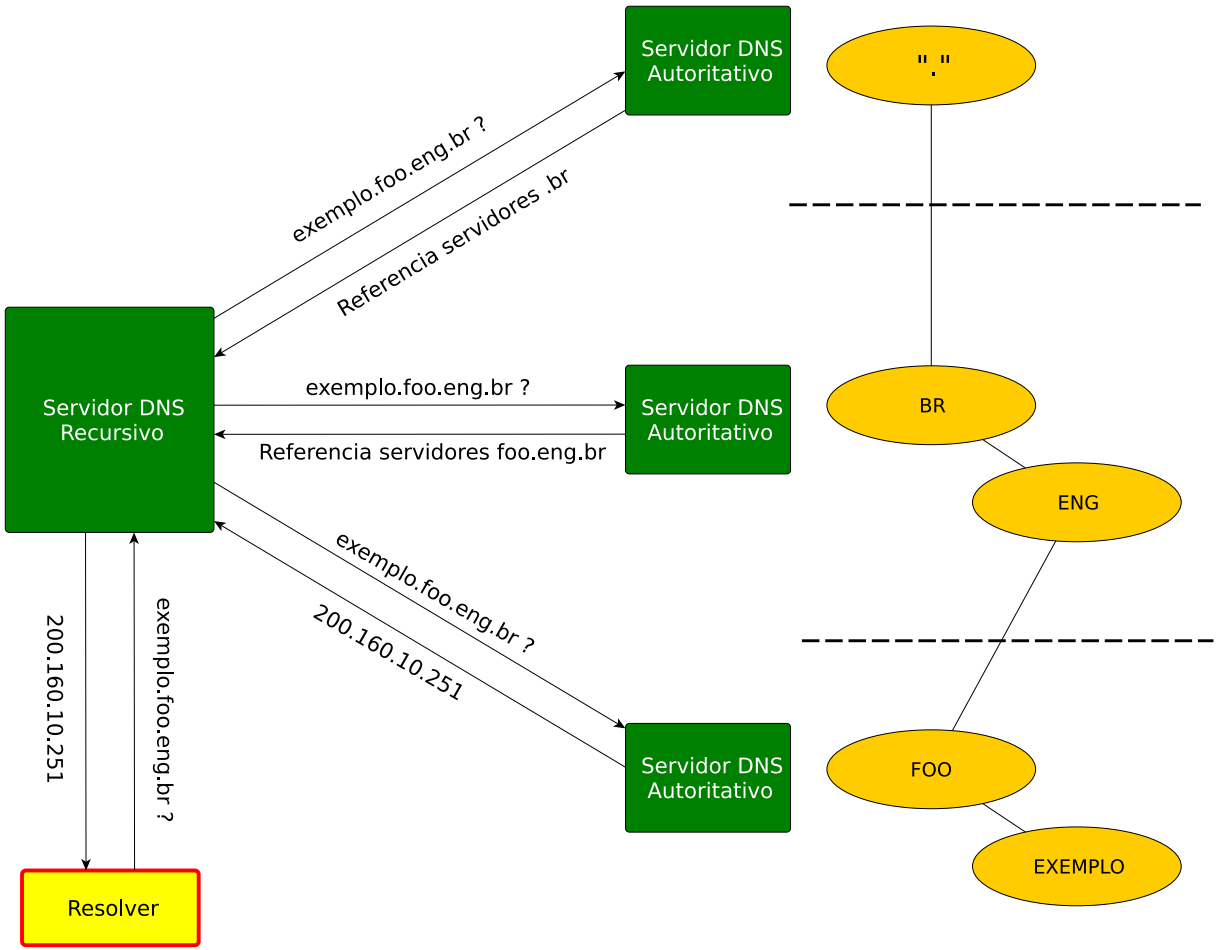
Exemplo de requisição de endereço



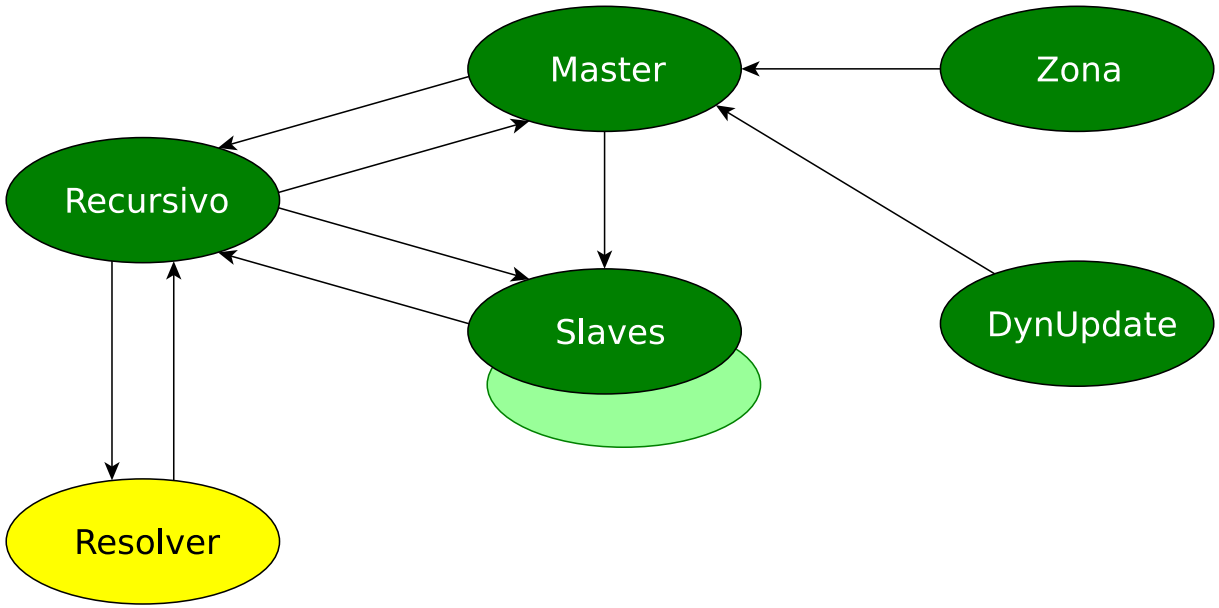
Exemplo de requisição de endereço



Exemplo de requisição de endereço

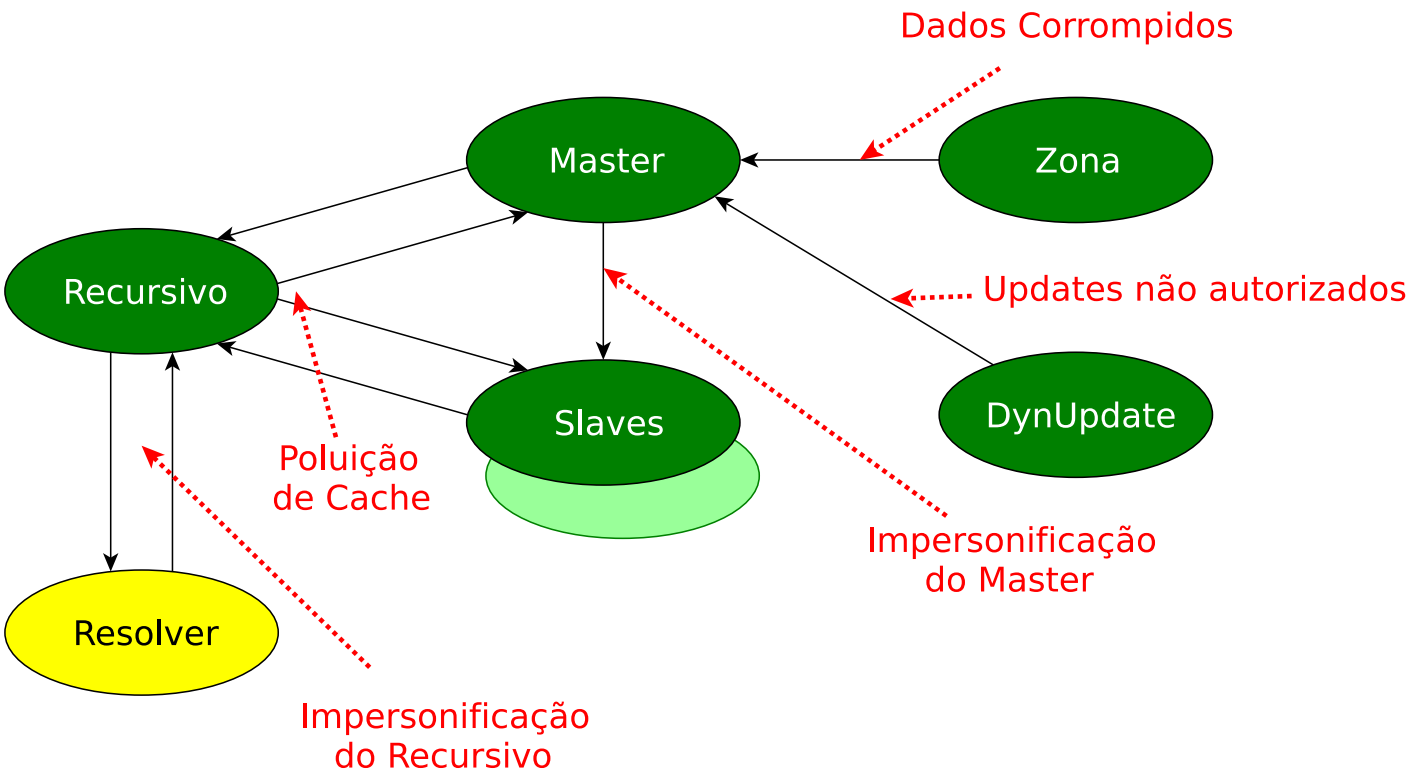


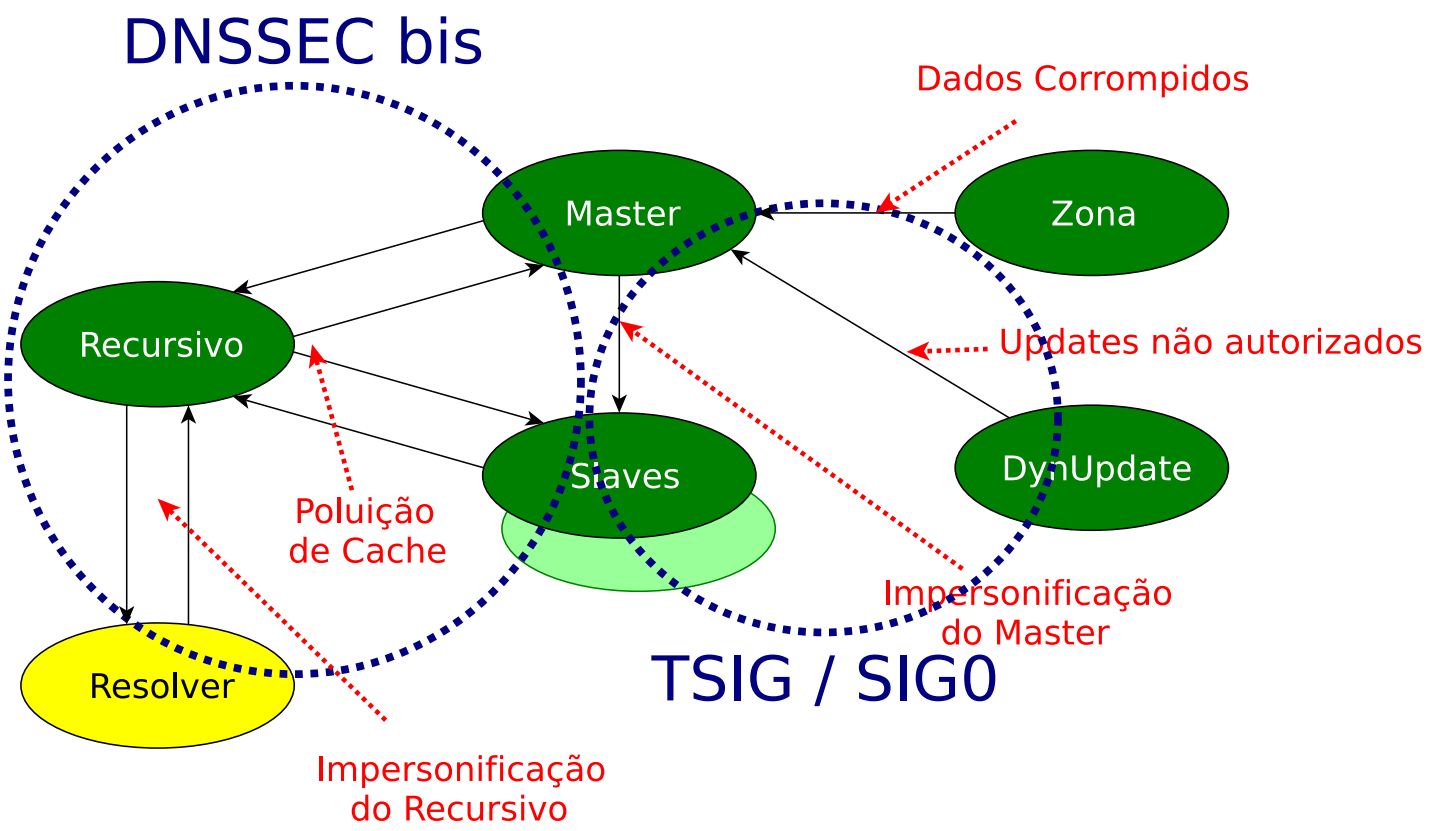
Fluxo de dados



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)

Vulnerabilidades

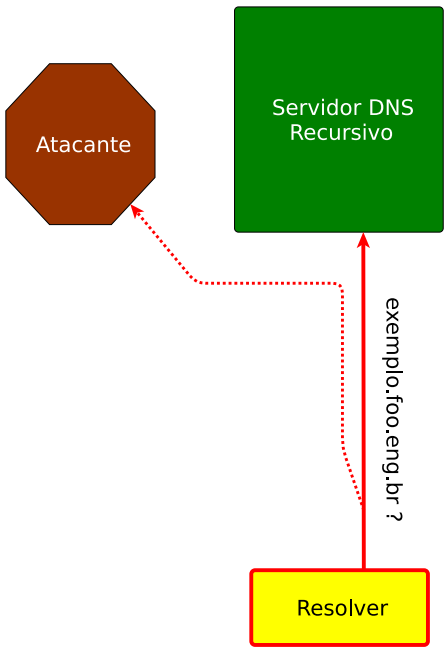



DNSSEC bis
Dados Corrompidos
Master
Zona
Recursivo
Updates não autorizados
Slaves
DynUpdate
Poluição
de Cache
Impersonificação
do Master
TSIG / SIG0
Resolver
Impersonificação
do Recursivo

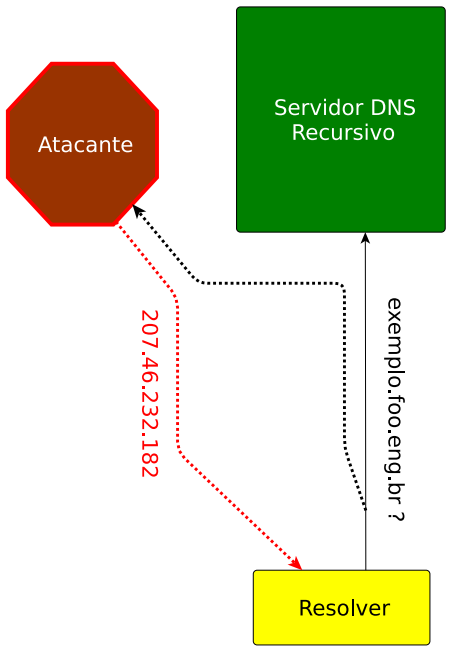
Exemplo de Ataque

Resolver

Exemplo de Ataque

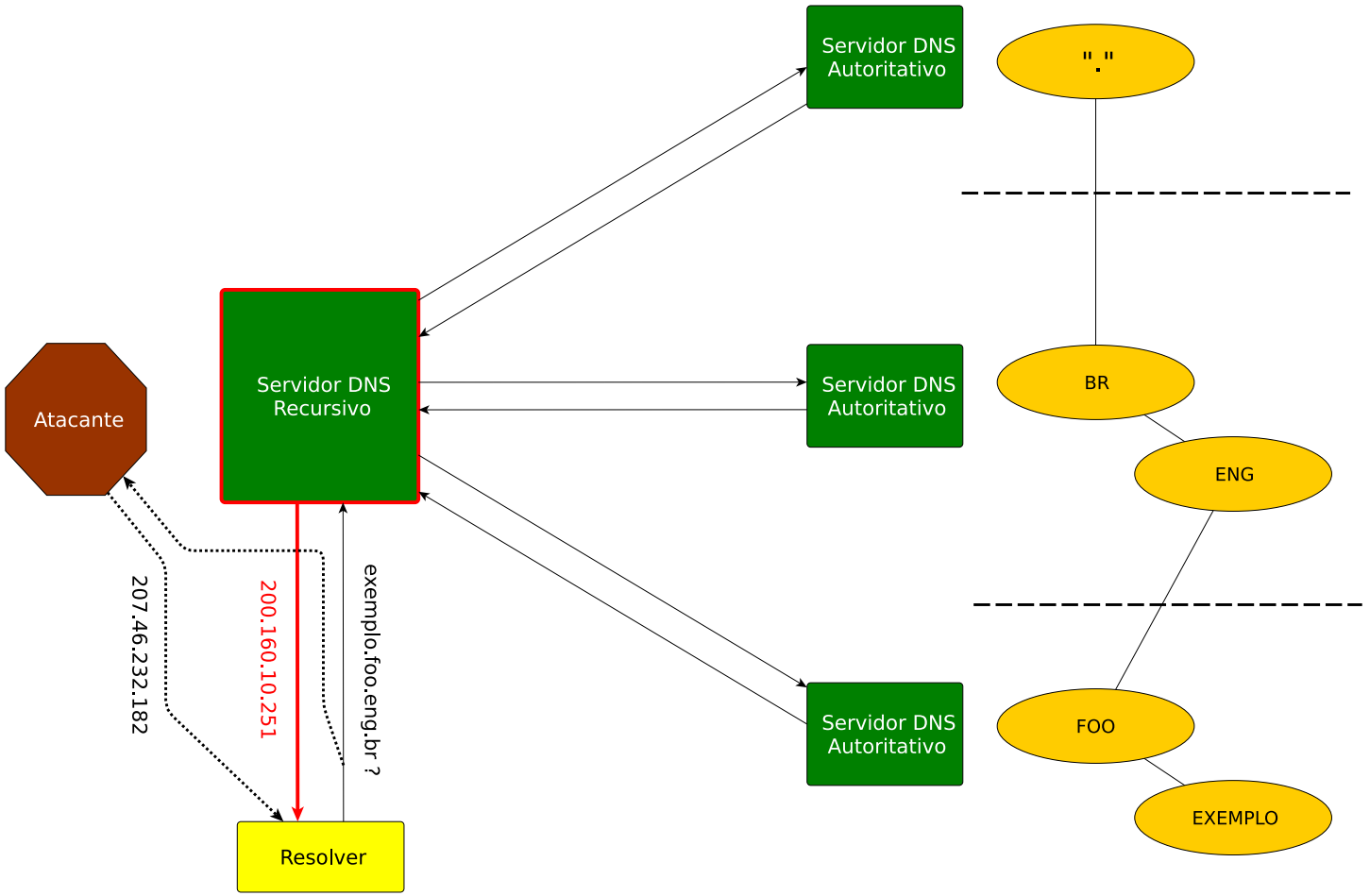


Exemplo de Ataque



O atacante responde mais rápido, spoofando endereço do resolver

Exemplo de Ataque



O atacante responde mais rápido, spoofando endereço do resolver

Ambientes Propícios

Segmentos compartilhados L2 ponto-multiponto

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

Ambientes Propícios

Segmentos compartilhados L2 ponto-multiponto

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

Atenção muito cuidado em conferências !

TSIG

Transaction Signatures – RFC 2845

- Autorização de AXFR (atualização total), IXFR (atualização das modificações) e Dynamic Updates (atualização imediata)
- Autenticação do servidor cache forwarder
- Tráfego assinado com a chave compartilhada

Soluções

registro.br
Registro de Domínios para a Internet no Brasil

TSIG

Transaction Signatures – RFC 2845

- Autorização de AXFR (atualização total), IXFR (atualização das modificações) e Dynamic Updates (atualização imediata)
- Autenticação do servidor cache forwarder
- Tráfego assinado com a chave compartilhada

DNSSEC

- Provê segurança para a resolução de endereços
- Funciona como um caminho alternativo para a verificação de autenticidade
- Suas verificações ocorrem antes de diversas aplicações de segurança (SSL, SSH, PGP, etc...)

nic.br

DNSSEC

Domain Name System SECurity extensions

- Extensão da tecnologia DNS
  (o que existia continua a funcionar)
- Possibilita maior segurança para o usuário na Internet
  (corrige falhas do DNS)
- Atualmente em sua segunda versão denominada DNSSEC bis

Garantias de DNSSEC

registro.br
Registro de Domínios para a Internet no Brasil

O que garante?

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

nic.br

Garantias de DNSSEC

registro.br
Registro de Domínios para a Internet no Brasil

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)

nic.br

registro.br
Registro de Domínios para a Internet no Brasil

Quem pode utilizar DNSSEC?

Os registros que estiverem diretamente abaixo dos domínios `.BR`, `.B.BR`, `.BLOG.BR`, `.ENG.BR`, `.ETI.BR` e `.GOV.BR`

Utilização de DNSSEC

registro.br
Registro de Domínios para a Internet no Brasil

Quem pode utilizar DNSSEC?

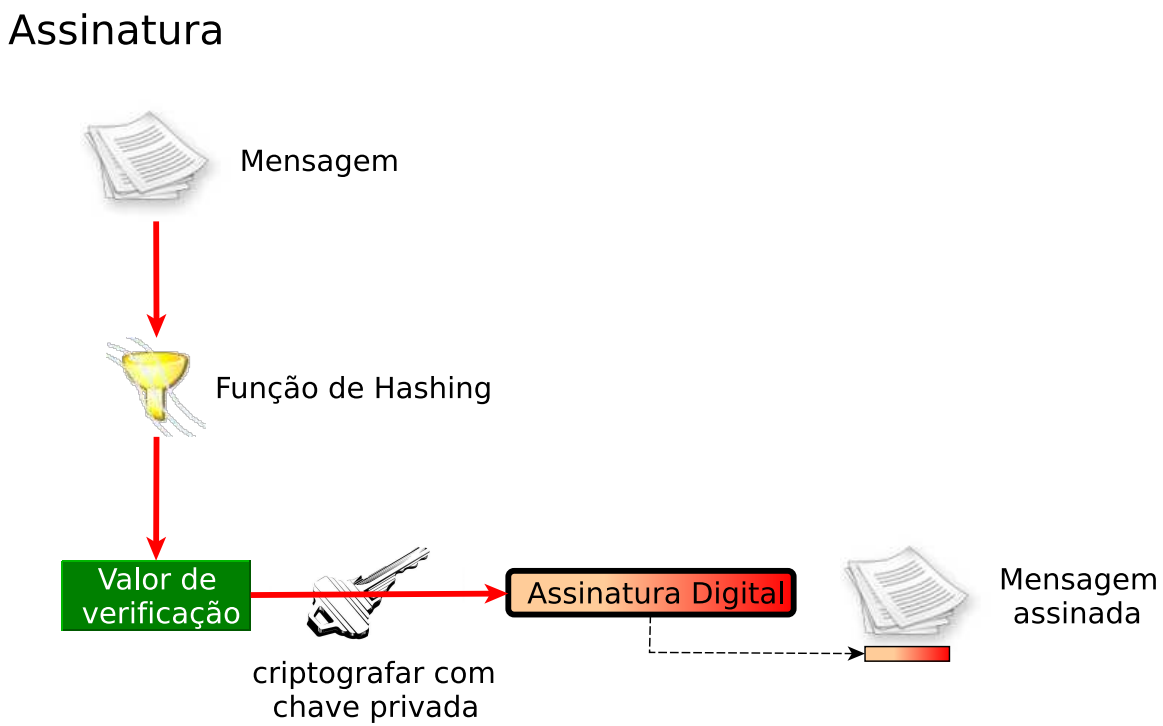
Os registros que estiverem diretamente abaixo dos domínios `.BR`, `.B.BR`, `.BLOG.BR`, `.ENG.BR`, `.ETI.BR` e `.GOV.BR`

Onde DNSSEC é Obrigatório?

É obrigatório nos registros que estiverem diretamente abaixo do domínio `.B.BR`

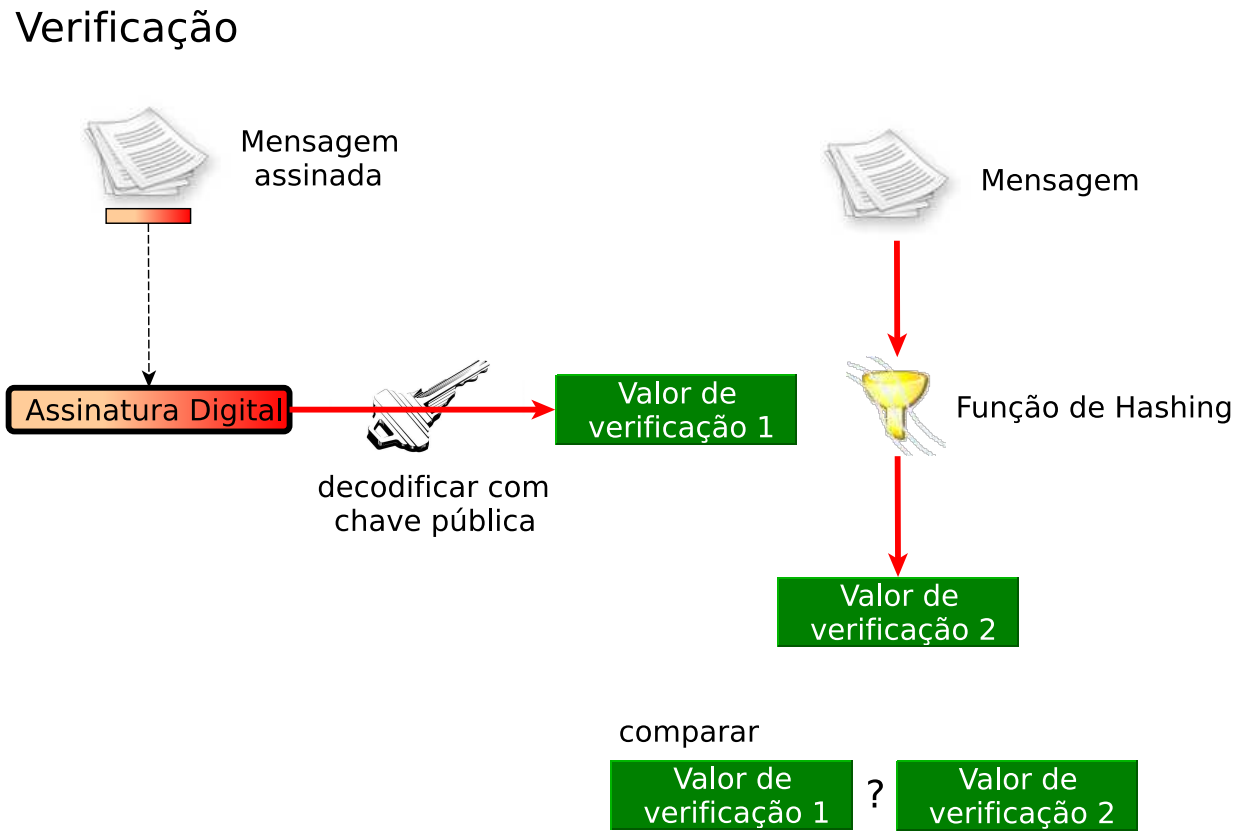
nic.br

Chaves Assimétricas



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

Chaves Assimétricas



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

Novos Resource Records

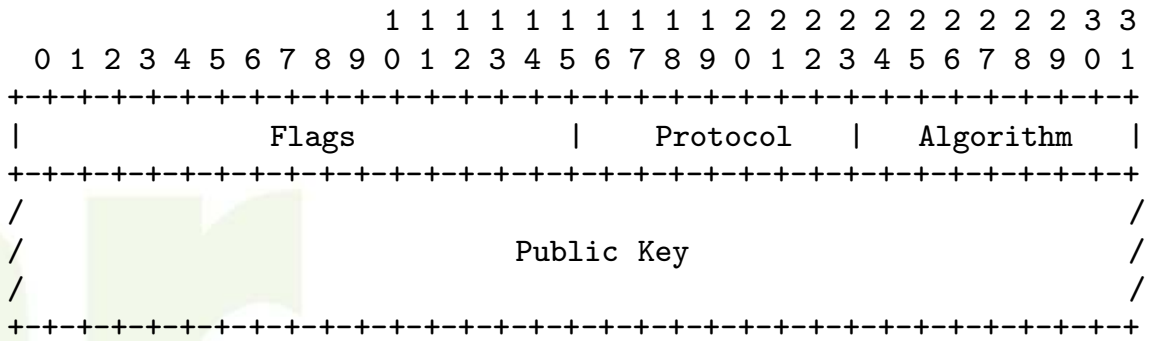
registro.br
Registro de Domínios para a Internet no Brasil

DNSKEY	Chave pública
RRSIG	Assinatura do RRset (somente registros com autoridade)
DS	Delegation Signer (Ponteiro para a cadeia de confiança)
NSEC	Aponta para o próximo nome e indica quais os tipos dos RRsets para o nome atual

nic.br

DNSKEY

É um resource record que armazena a chave pública da zona

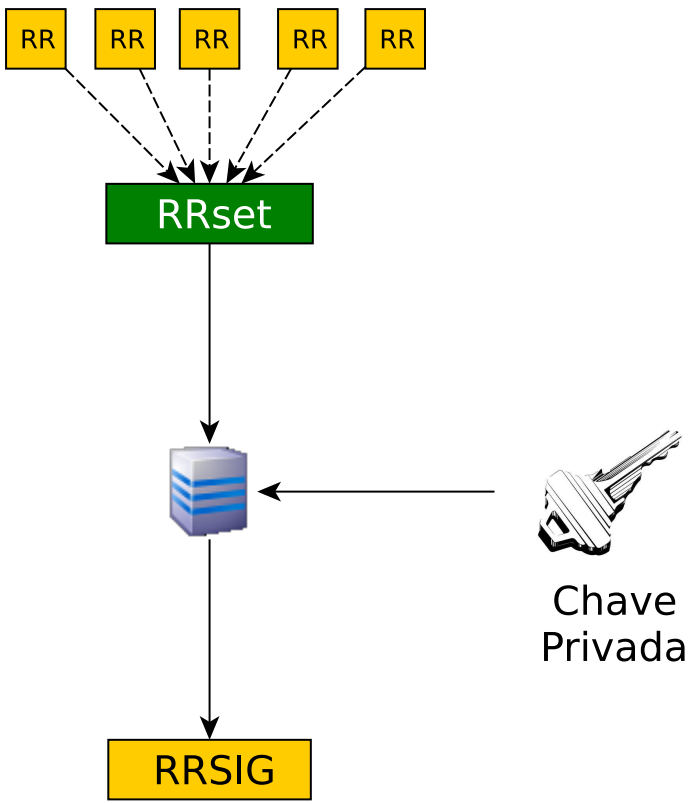


Exemplo

```
foo.eng.br.          900 IN DNSKEY 256 3 5 (
                            AwEAAeZPN2yMs9q6kgYjFUblEwjCnWWcPq+TGcJrD5ga
                            XXAbP5MAqIkgZ5J4TU1mmpL1A8gMfd/wUmBkVipXR8FK
                            HRajBZSRfgeKnKaQtrxNZ32Ccts2F6Ylv9WaLXtiqebg
                            OZtuJFpQr6pnIt/FoOI+I7BUSNrX28VTq4jXu/qTrmM/
                            ) ; key id = 62745
```

RRSIG

- É um resource record que contém a assinatura de um RRset específico com uma determinada chave (DNSKEY)
- Possui uma validade inicial (inception) e final (expiration)



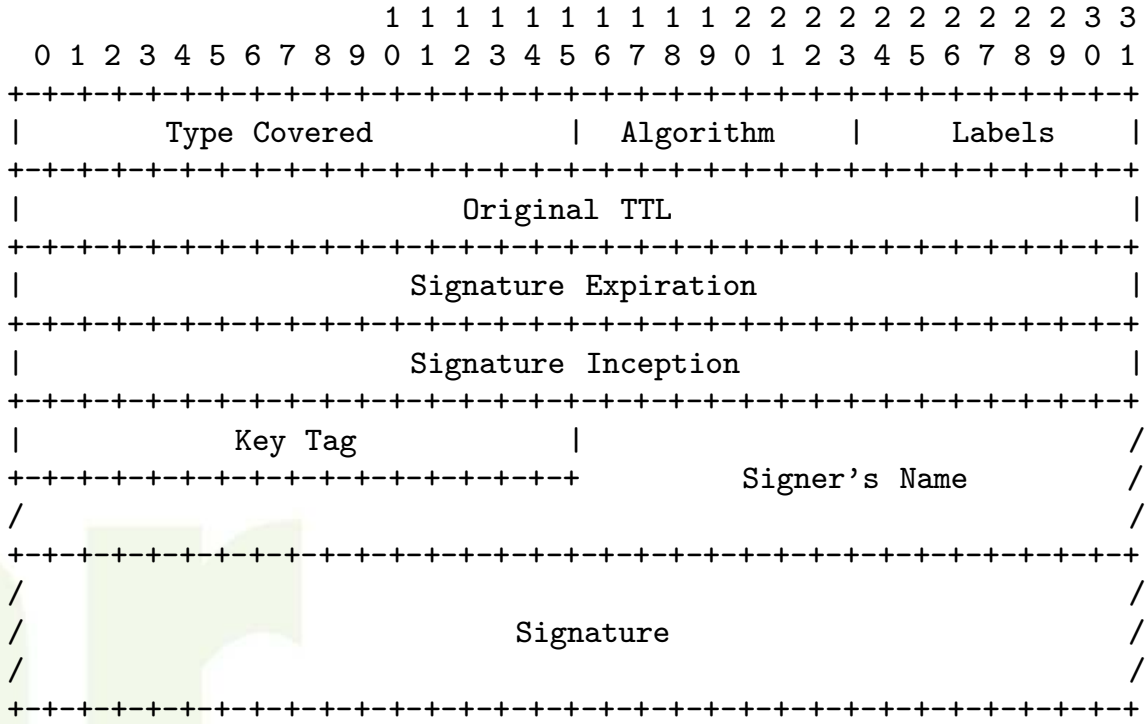
Exemplos de RRset:

```
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
```

RRSIG



Exemplo

```
foo.eng.br.          900 IN RRSIG SOA 5 3 900 20070617200428 (
                            20070518200428 62745 foo.eng.br.
                            glEeCYyd/CCBfzH64y0RAQf9OxYDsI4xuBNaam+8DZQZ
                            xeoSLQEEtwmp6wBtQ7G10wSM9nEjRRhbZdNPNKJMp2PE
                            lLLgLI+BLwdlz0t8MypcpLOaTm9rc7pP7UR5XLzU1k8D
                            m6ePW1bNkId7i0IPSghyoHM7tPVdL2GW51hCujA= )
```

É um hash do Record DNSKEY

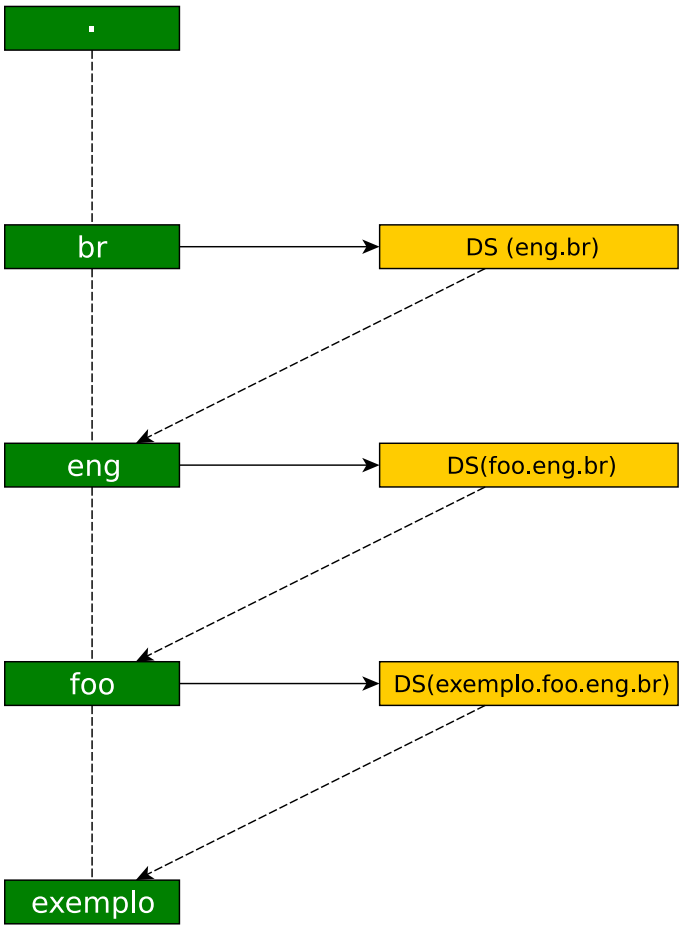
Serve para informar que existem uma cadeia de confiança entre um domínio e seus sub-domínios.

Indica:

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

A zona Pai tem autoridade pelo registro DS

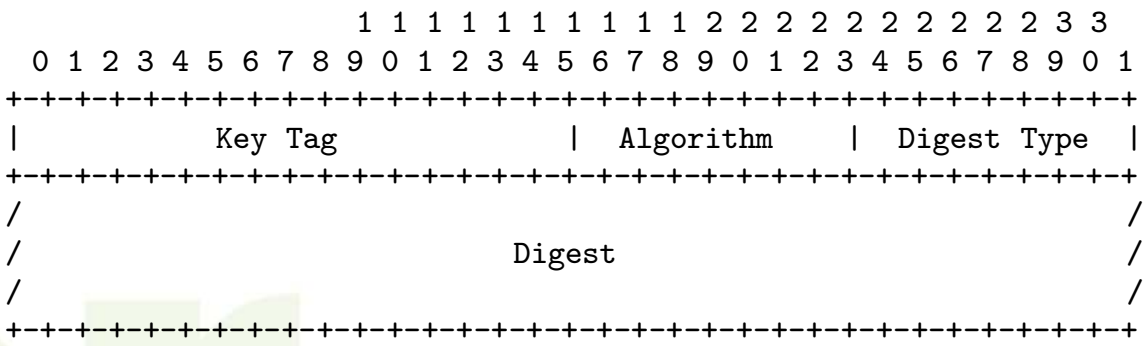
- Os registros NS são apenas "hints" e não são autoritativos no Pai
- O record DS **não** deve aparecer no Filho



Cadeia de Confiança

O Record DS é um ponteiro para a cadeia de confiança, a qual garante a autenticidade das delegações de uma zona até um ponto de confiança – uma chave ancorada ou a utilização de DLV

DS



Exemplo

```
foo.eng.br.             IN DS 817 5 1 EAEC29E4B0958D4D3DFD90CC70C6730AD5880DD3
```

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

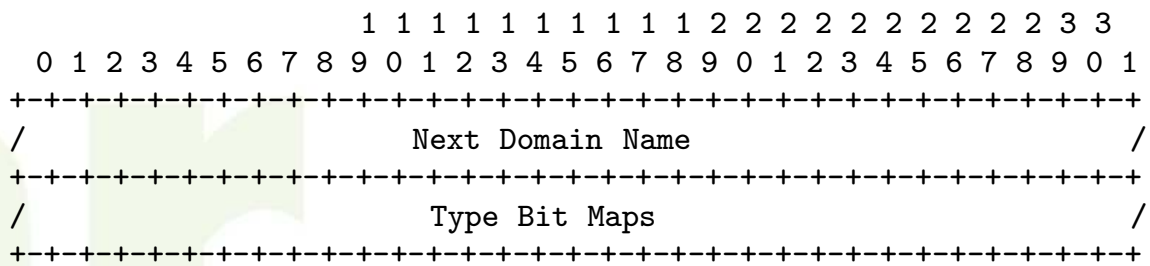
Exemplo de DS pelo Whois

```
$ 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
```

NSEC - Next Secure

Permite autenticar uma resposta negativa

- Próximo nome seguro
- Indica os tipos de RRsets existentes
- Último registro da zona aponta para o primeiro (SOA)



Exemplo

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

Prova de não existência, com pré-assinatura, sem a necessidade de chaves on-line para assinatura on-demand. Diminuindo a possibilidade de DOS.

NSEC - Simulação nome não existente

- 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/CCBfzH64y0RAQf9OxYDsI4xuBNaam+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/p1dLmAT7NF5Rkc
                               9IfbAHZTxefoqTKqN/vPl1PqSxUzh0rl+atHblaH6yt79CTkmStota7C
                               SLYYXX5c7D93hRYJ2yk1COxQz6GG9SIp/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+EhQYohuimuwk1xzAemsn292esUhkkYz/BG7b
                               OT/L9fhzOEPYtYGFyMF4gZ1/mxwY31UmX6xVZZPYFJ7x5Kw2uTSD49FK
                               VsdUOLBCAHzO88byAm8EwLe3l+U0/q8RvPimAfpouoivUDcuWtKxs0CzLyc=
```

NSEC - Simulação tipo não existente

- 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/CCBfzH64y0RAQf9OxYDsI4xuBNaam+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/p1dLmAT7NF5Rkc
                            9IfbAHZTxefoqTKqN/vPl1PqSxUzh0rl+atHblaH6yt79CTkmStota7C
                            SLYYXX5c7D93hRYJ2yk1COxQz6GG9SIp/U4qR4//TcQDHpqQ4bFs42ZsD4I=
```

NSEC - Simulação nome existente

Record NSEC utilizado apenas para provar não existência. Não aparece em consultas "positivas"

```
$ 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/CCBfzH64y0RAQf9OxYDsI4xuBNaam+8DZQZxeoSLQEEtwmp
                             6wBtQ7G10wSM9nEjRRhbZdNPNKJMp2PElLLgLI+BLwdlz0t8MypcpLOa
                             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+UeqYk0xgQGQQXkBzcKiKQRPwe+1JZlpjEzjU1Uj0HUOHefa
                             jXzMv7FlFMWYeU51Ybg49HFe67XQVlK54GeAFXWB7YS59yODLoNEBxQl
                             9QEy6g/OOnLpuKTrST8qqd5Fc/eYqN/Ag3GnfcAviZgiQhhveGH9mJHWZyc=
```

Funcionamento

- Autenticidade e Integridade são providas pela assinatura dos Resource Records Sets (RRset) com uma chave privada
- Zonas delegadas (filhas) assinam seus RRsets com a chave privada
  - Autenticidade da chave é verificada pela assinatura na zona pai do Record DS (hash da chave pública – DNSKEY – da zona filha)
- Chave pública é usada para verificar assinatura (RRSIGs) dos RRsets
- Autenticidade da não existência de um nome ou tipo provida por uma cadeia de nomes (NSEC) que aponta para o próximo nome em uma sequência canônica

DNSSEC não é PKI

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

Ancorar Chave - Servidor Recursivo

Sempre que utilizar um Servidor Recursivo com DNSSEC habilitado é necessário ancorar a chave pública.

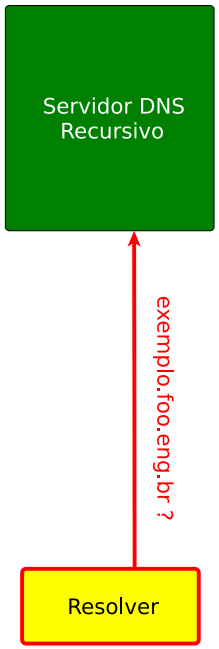
Isto serve para associar o inicio da cadeia de confiança a um ponto seguro.

Obtendo a chave a ser ancorado da zona ".br"

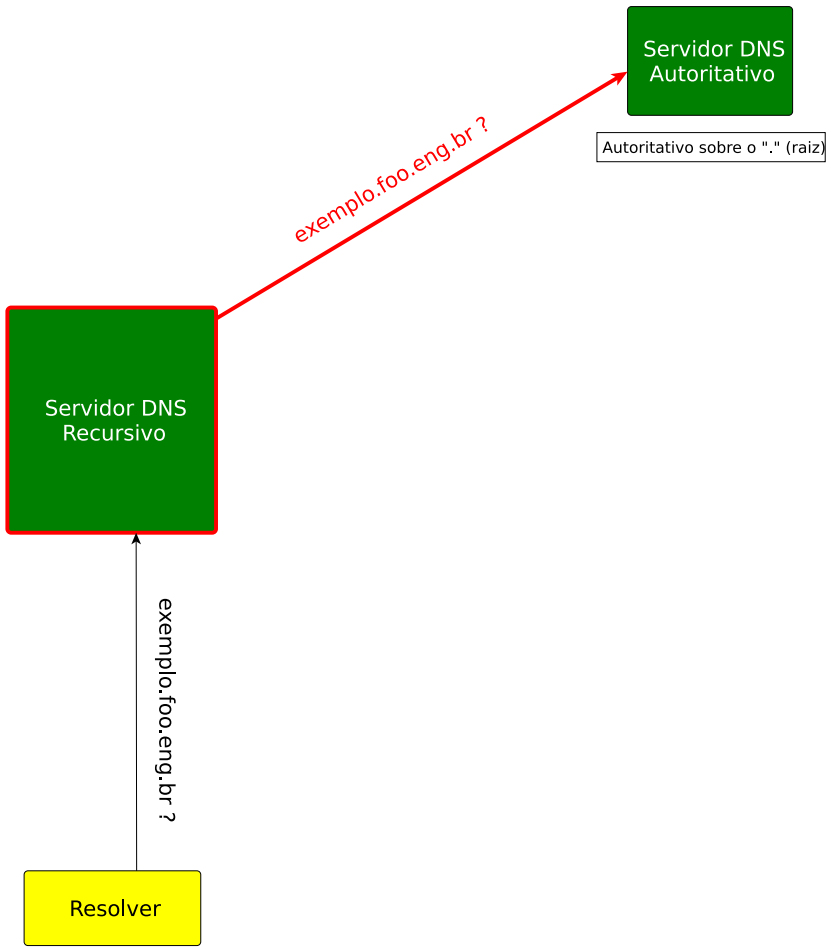
- **.BR** `https://registro.br/ksk/`

Exemplo

- O resolver recursivo já possui a chave pública da zona ".br" ancorada

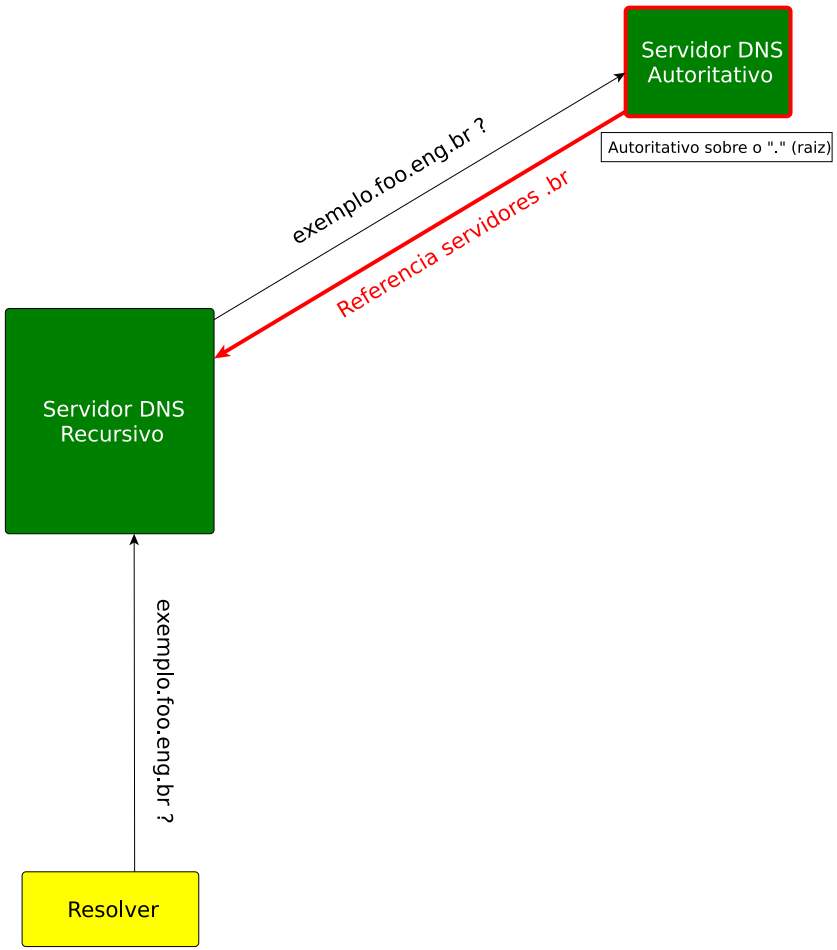


Exemplo



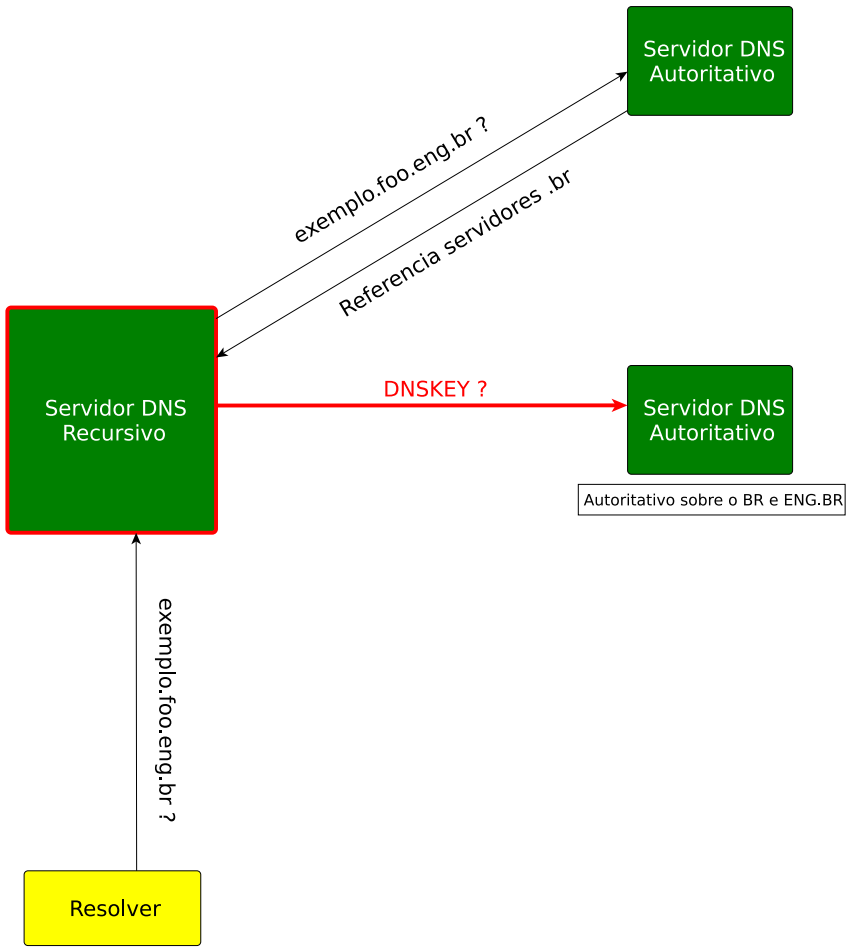
- Nesta simulação de resolução supomos que a raiz não está assinada.

Exemplo



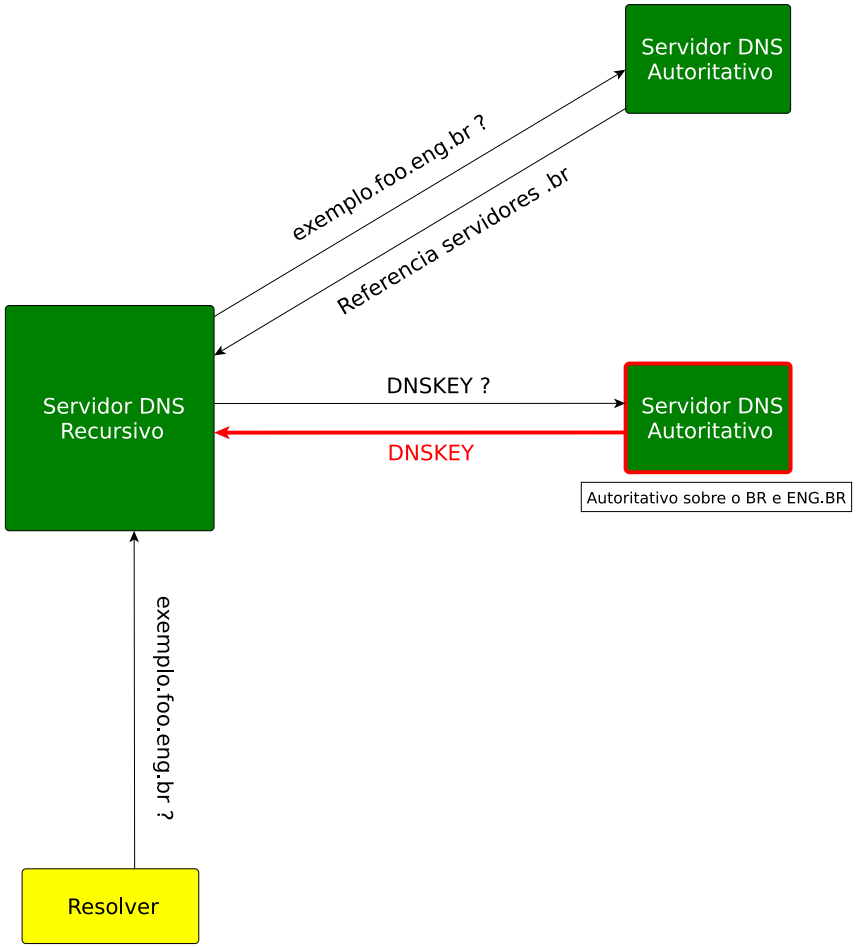
- Retorna sem resposta, mas com referência para os Records: NS do “.br”.

Exemplo



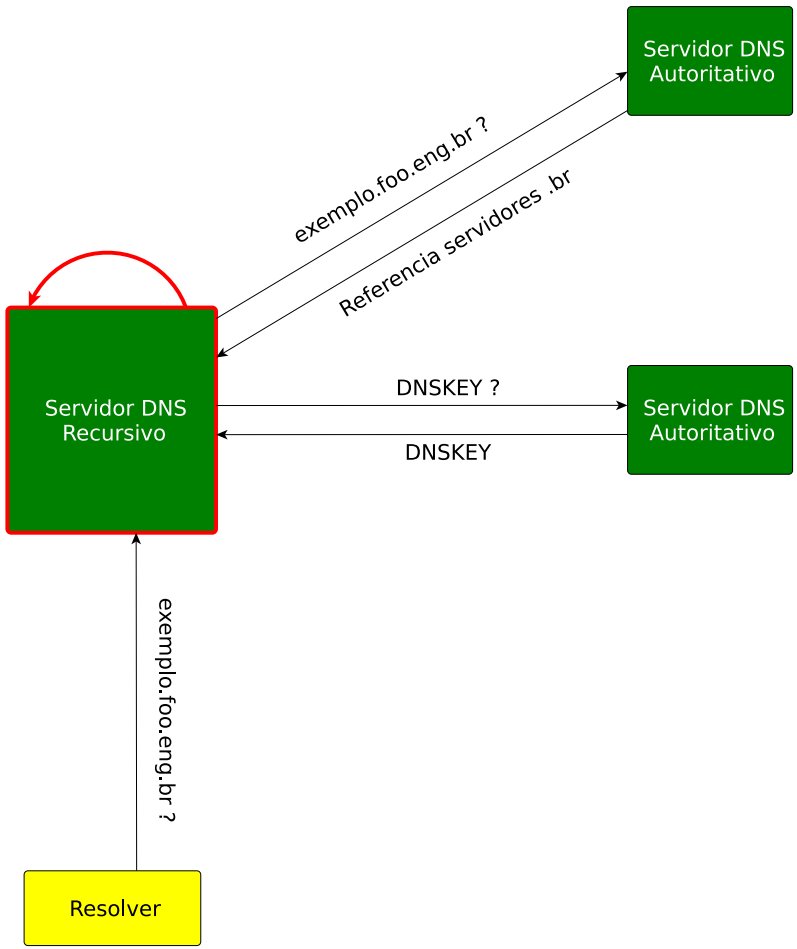
- O servidor recursivo requisita a DNSKEY ao verificar que o nome da zona é igual ao nome da zona que consta em sua trusted-key.

Exemplo



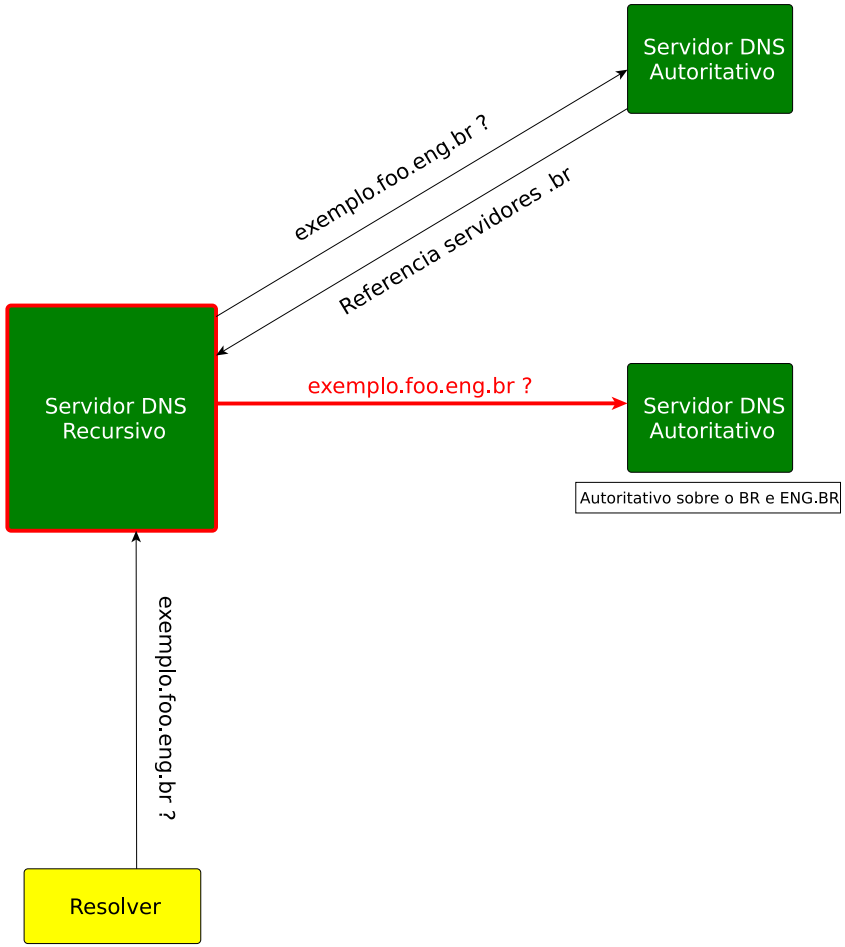
- O servidor DNS responde enviando DNSKEY e o RRSIG

Exemplo

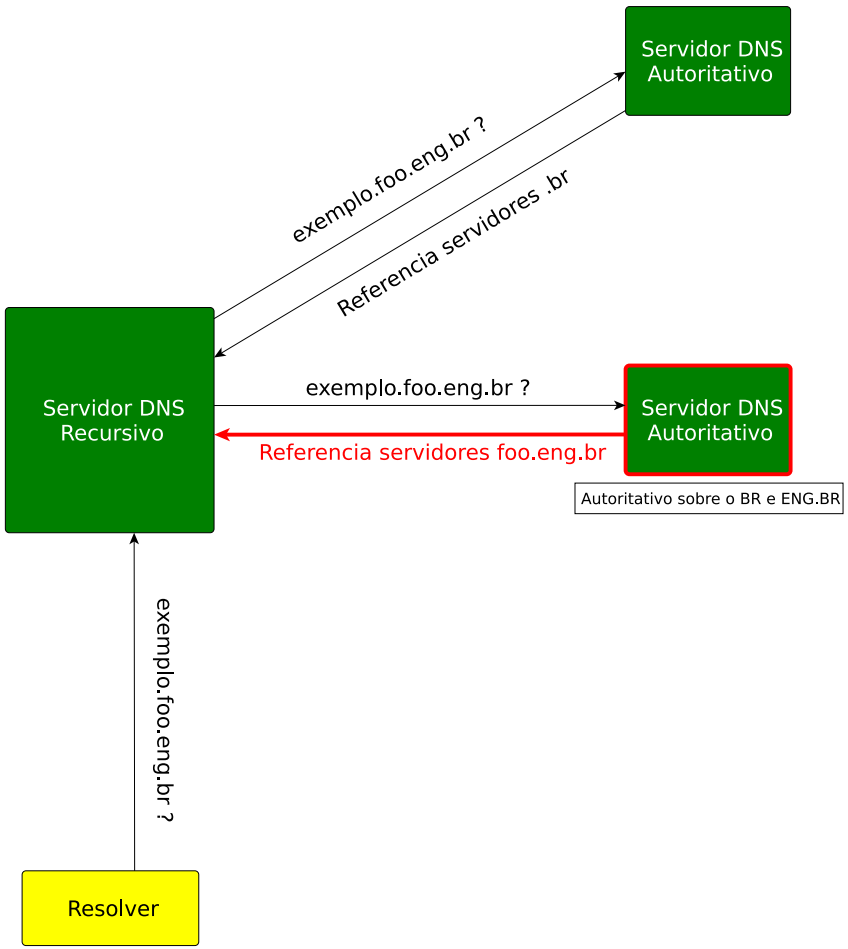


- Compara a trusted-key com a DNSKEY, caso for válida continua com as requisições

Exemplo


Servidor DNS
Autoritativo
exemplo.foo.eng.br ?
Referencia servidores .br
Servidor DNS
Recursivo
exemplo.foo.eng.br ?
Servidor DNS
Autoritativo
Autoritativo sobre o BR e ENG.BR
exemplo.foo.eng.br ?
Resolver

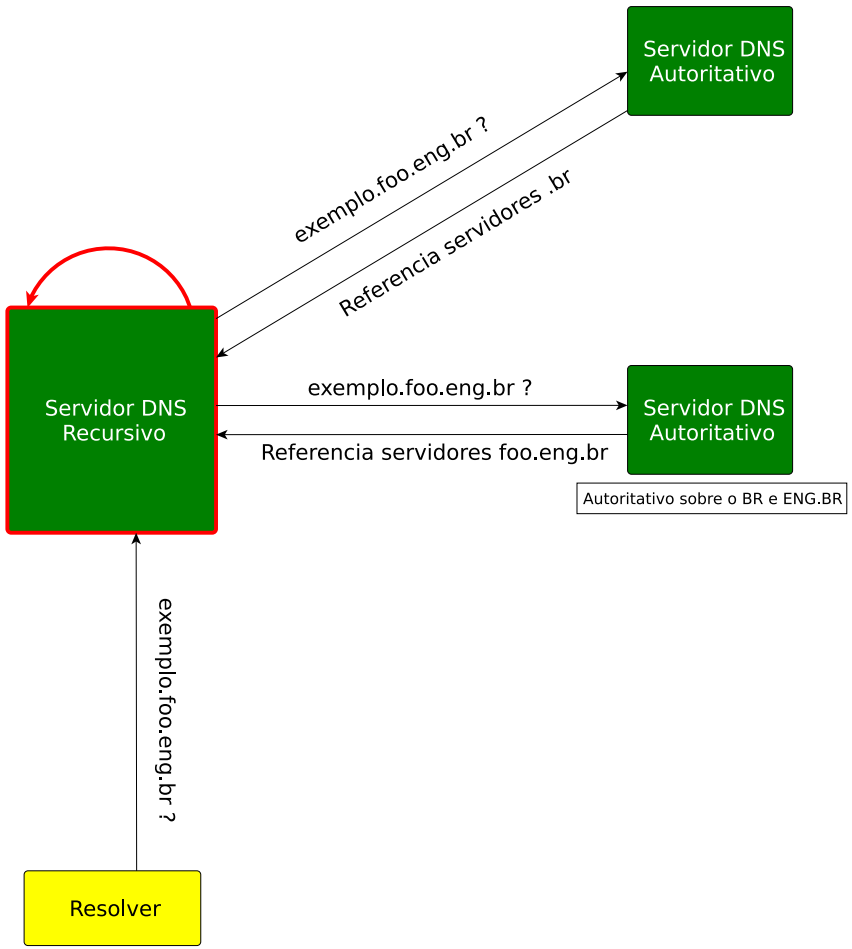
Exemplo



- Retorna sem resposta, mas com referência para os Records:
  - NS do "foo.eng.br"

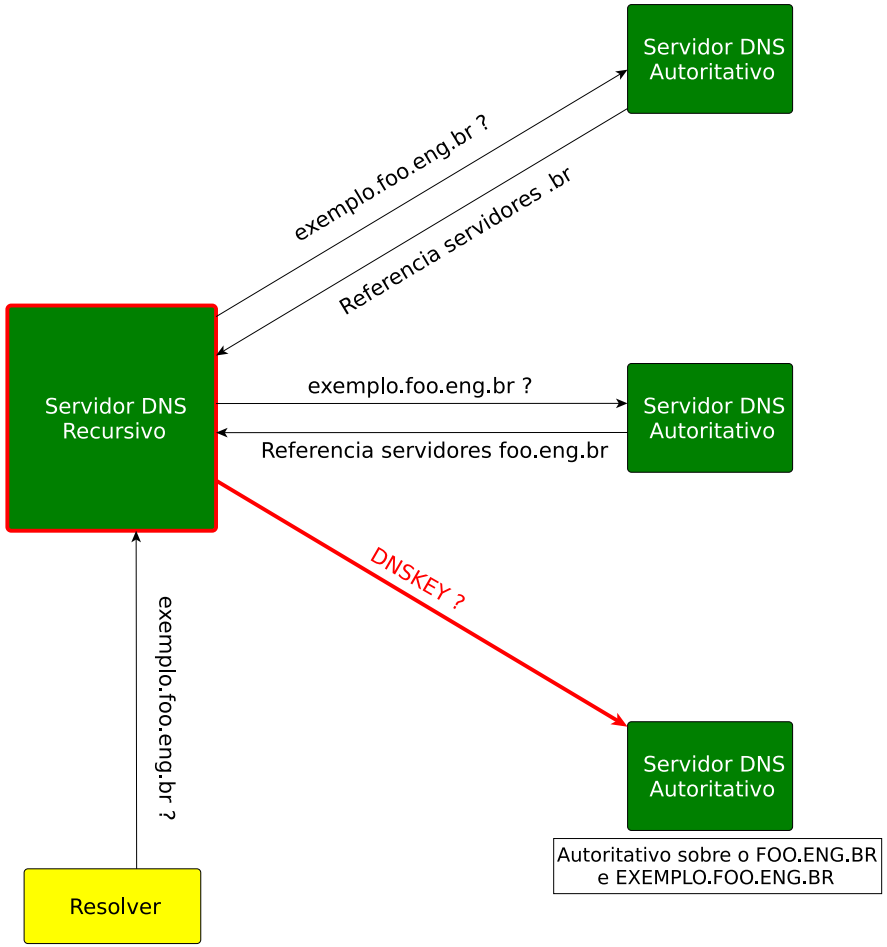
  e com autoridade sobre os Records:
  - DS do "foo.eng.br"
  - RRSIG do Record DS

Exemplo

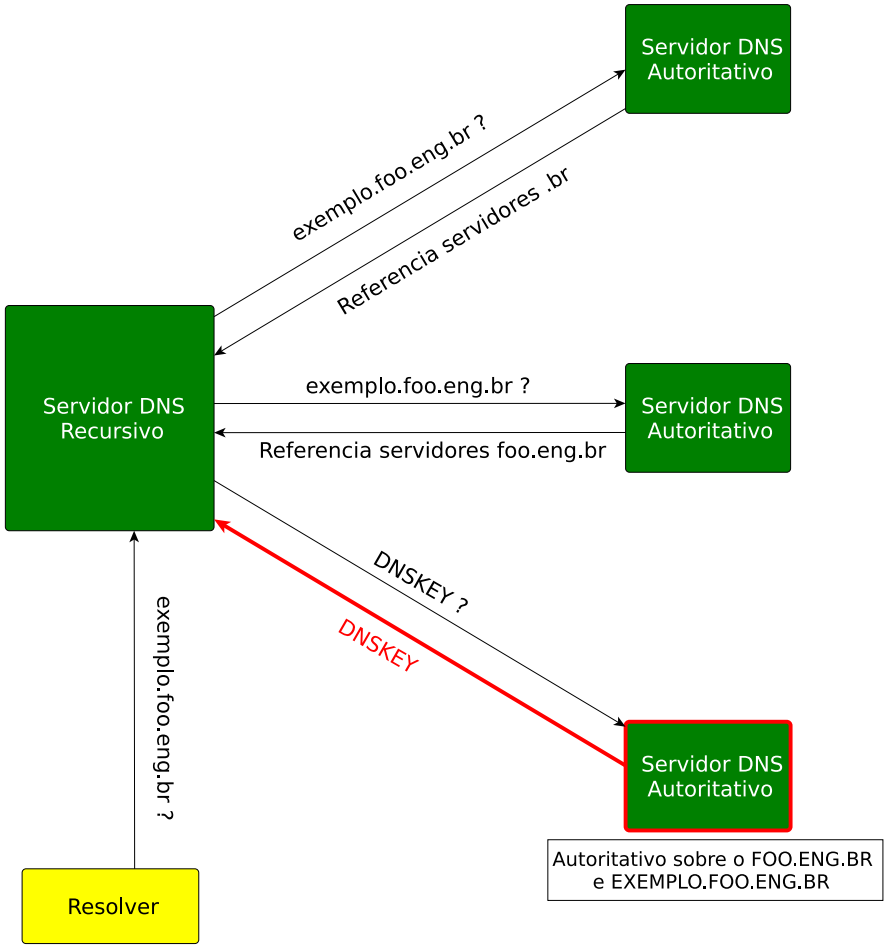


- O servidor DNS recursivo utiliza a DNSKEY para checar a assinatura (RRSIG) do Record DS

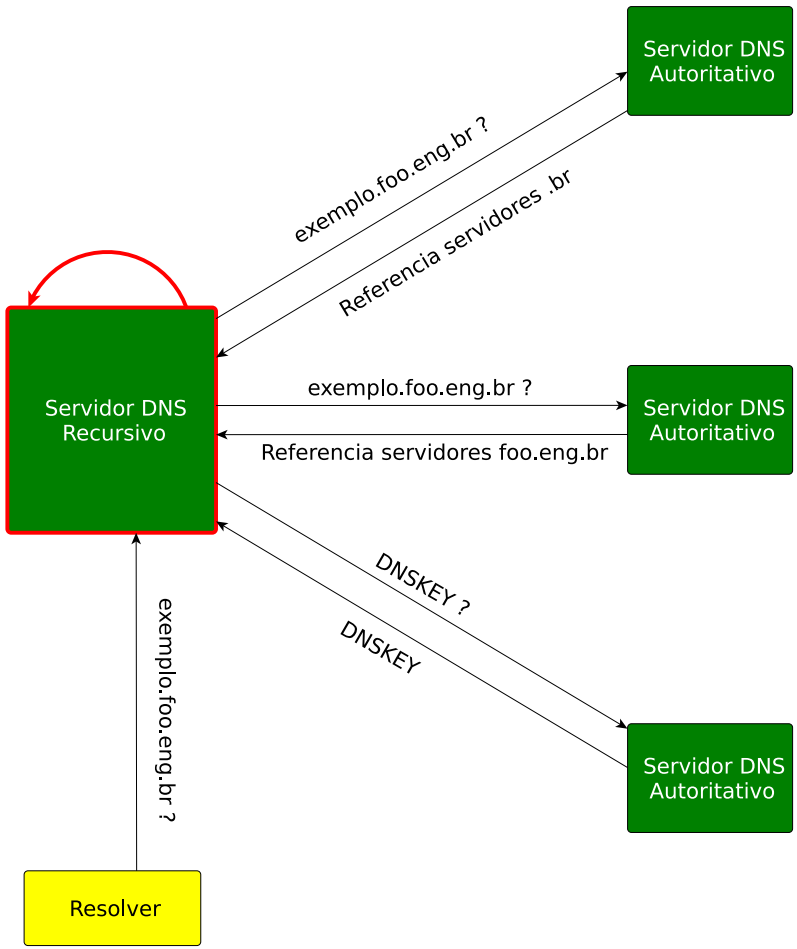
Exemplo


Servidor DNS Autoritativo
exemplo.foo.eng.br ?
Referencia servidores .br
Servidor DNS Recursivo
exemplo.foo.eng.br ?
Servidor DNS Autoritativo
Referencia servidores foo.eng.br
DNSKEY ?
exemplo.foo.eng.br ?
Servidor DNS Autoritativo
Autoritativo sobre o FOO.ENG.BR e EXEMPLO.FOO.ENG.BR
Resolver

Exemplo

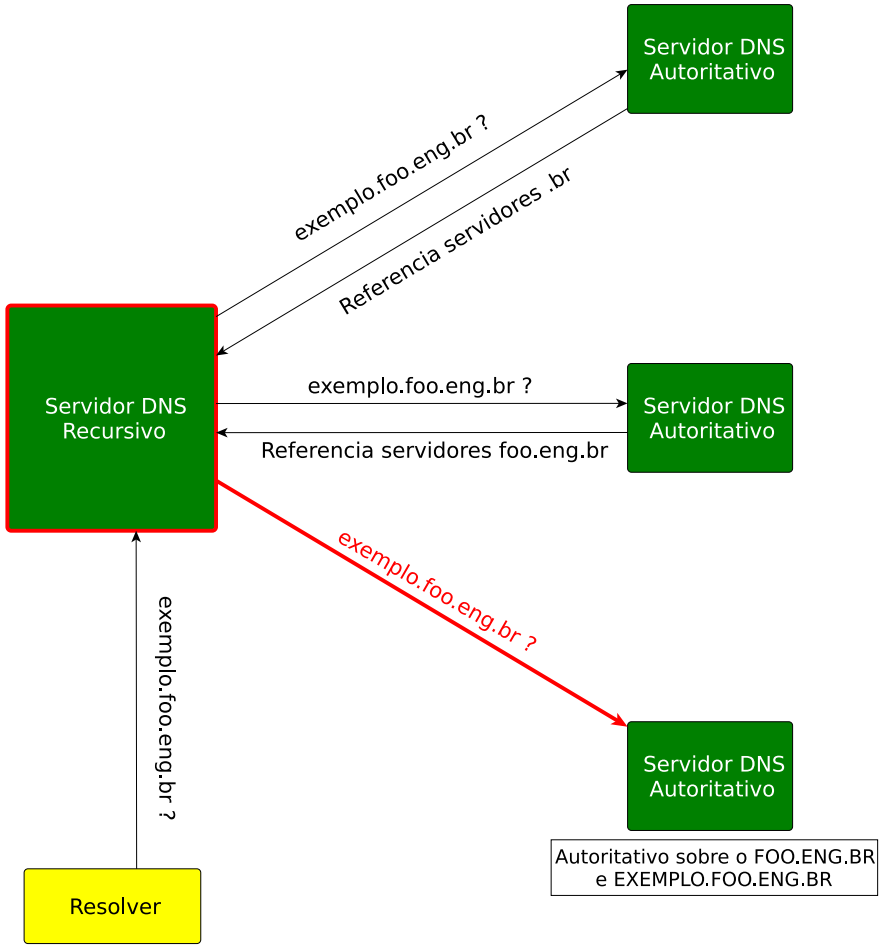

Servidor DNS Autoritativo
exemplo.foo.eng.br ?
Referencia servidores .br
Servidor DNS Recursivo
exemplo.foo.eng.br ?
Servidor DNS Autoritativo
Referencia servidores foo.eng.br
DNSKEY ?
DNSKEY
exemplo.foo.eng.br ?
Servidor DNS Autoritativo
Autoritativo sobre o FOO.ENG.BR e EXEMPLO.FOO.ENG.BR
Resolver

Exemplo



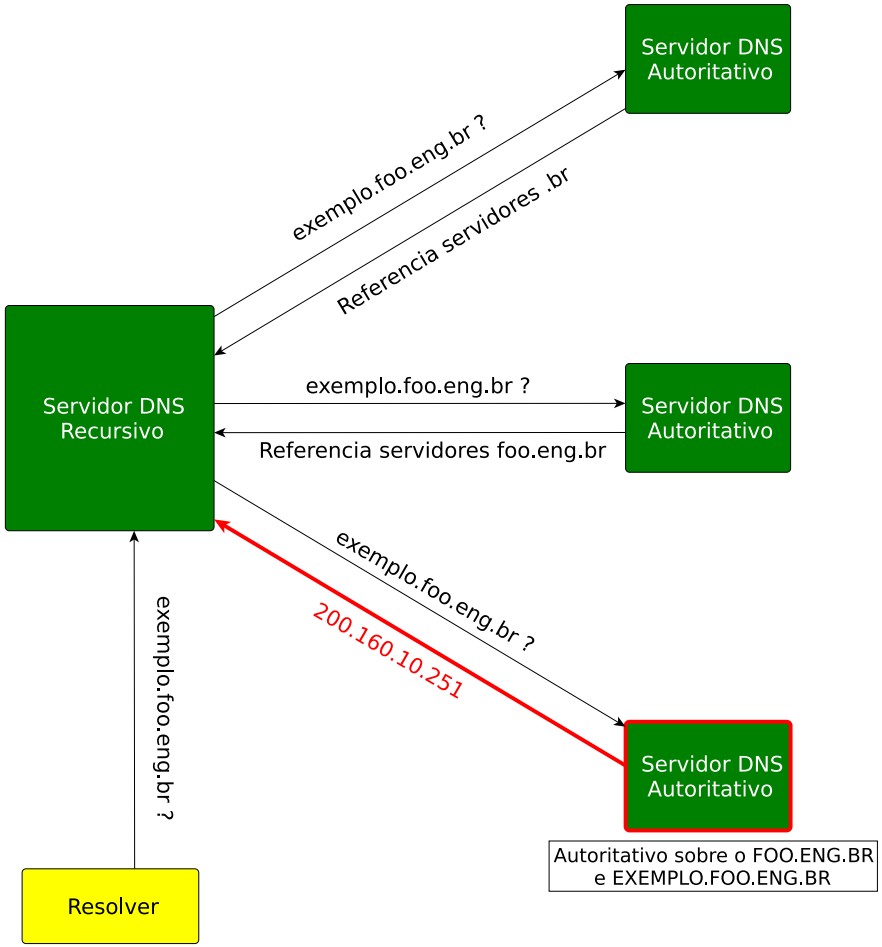
- O servidor DNS recursivo verifica através do DS e da DNSKEY, se este servidor DNS é válido.

Exemplo

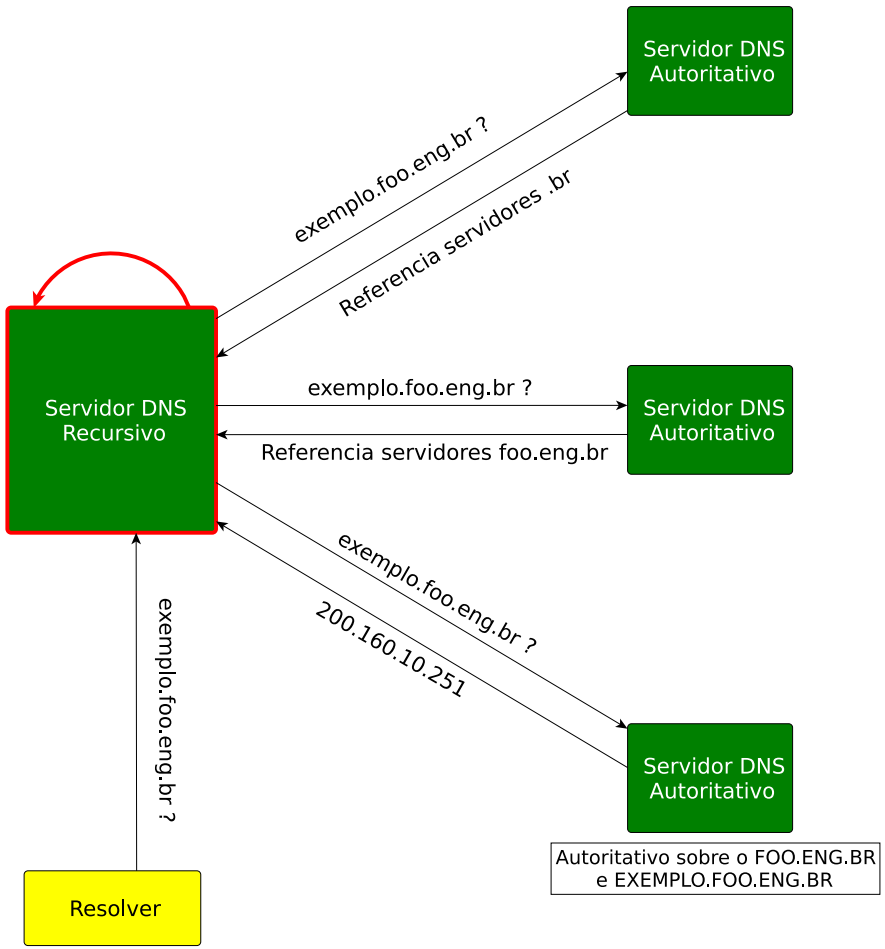

Servidor DNS Autoritativo
exemplo.foo.eng.br ?
Referencia servidores .br
Servidor DNS Recursivo
exemplo.foo.eng.br ?
Servidor DNS Autoritativo
Referencia servidores foo.eng.br
exemplo.foo.eng.br ?
exemplo.foo.eng.br ?
Servidor DNS Autoritativo
Autoritativo sobre o FOO.ENG.BR e EXEMPLO.FOO.ENG.BR
Resolver

Exemplo

- Retorna o Record A e sua assinatura RRSIG.

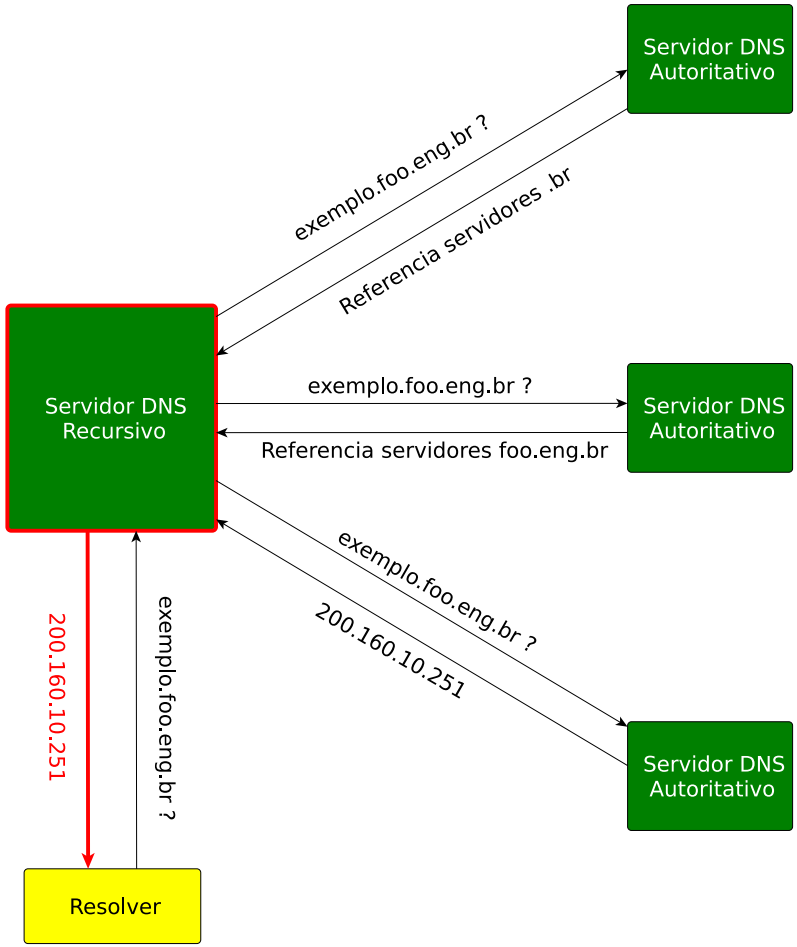


Exemplo



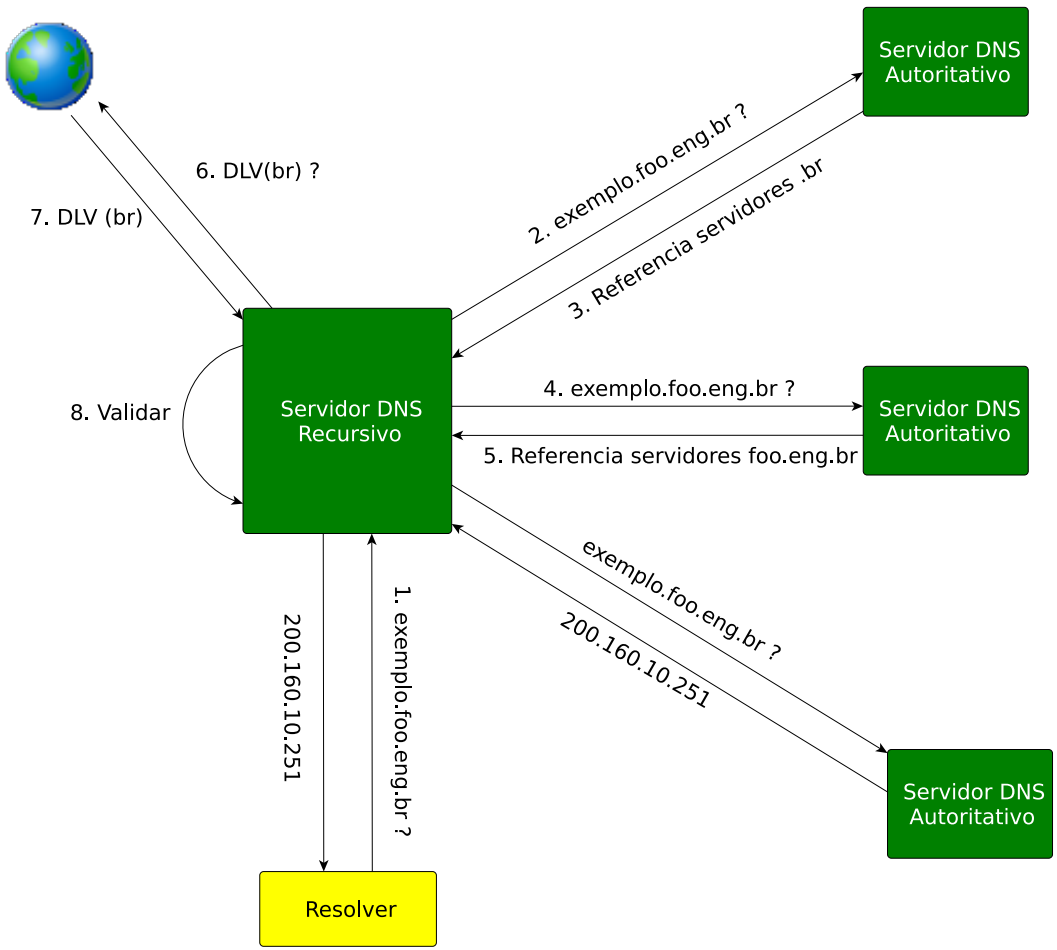
- O servidor DNS recursivo utiliza a DNSKEY para checar a assinatura (RRSIG) do Record A

Exemplo


Servidor DNS Autoritativo
exemplo.foo.eng.br ?
Referencia servidores .br
Servidor DNS Recursivo
exemplo.foo.eng.br ?
Servidor DNS Autoritativo
Referencia servidores foo.eng.br
exemplo.foo.eng.br ?
200.160.10.251
200.160.10.251
exemplo.foo.eng.br ?
Servidor DNS Autoritativo
Resolver

DLV – DNSSEC Lookaside Validation

Exemplo de chave não ancorada



- Permite que um domínio sem um pai assinado utilize DNSSEC

RFC 4431
The DNSSEC Lookaside Validation (DLV) DNS Resource Record

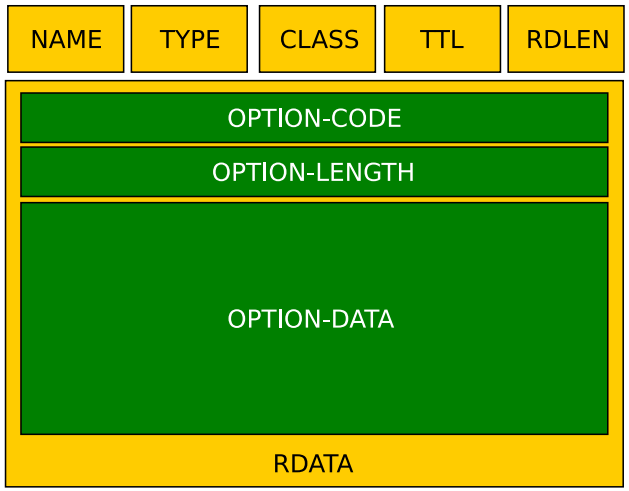
EDNS0 (RFC 2671)

Criado de forma a tornar mais flexíveis as limitações dos campos no protocolo DNS e possibilitar a analise de novos fatores na camada de transportes.

- Permite aos solicitadores informarem a capacidade máxima de seus pacotes UDP. Eliminando a limitação UDP DNS de 512 bytes.
- Aumenta a quantidade de flags e expande alguns campos já existentes no protocolo para permitir uma maior diversidade de valores
- É estruturado de forma a permitir o crescimento do protocolo
- Distingue quem suporta DNSSEC a partir da flag DO (DNSSEC OK, nova flag incluída nesta extensão)

Lembrete

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




```
NAME        ‘‘.’’
TYPE        ‘‘OPT’’
CLASS       Tamanho do pacote UDP
TTL         RCODE estendido e Flags
RDATA       Pares {Atributo, Valor}
```

Pseudo-RR OPT

- Armazena informações do EDNS0
- Não é armazenado em arquivo, sendo apenas utilizado no momento da comunicação entre os servidores

Configuração de Firewall

O firewall deve ser configurado para fazer a normalização de fragmentos de pacote UDP antes de checar as demais regras.

Caso isto não seja possível, uma alternativa é configurar o servidor recursivo para que solicite respostas UDP menores. Se estiver sendo utilizado Bind como servidor recursivo, isto pode ser feito a partir da versão 9.3.0 com a opção edns-udp-size:

```
options {
    edns-udp-size 1252;
};
```

Recomendação

Firewalls e DNS, como e porque configurar corretamente
ftp://ftp.registro.br/pub/doc/dns-firewall.pdf

Conceito de Chaves

registro.br
Registro de Domínios para a Internet no Brasil

Key Signing Key (KSK)

As chaves utilizadas para assinar as chaves da zona, sendo, assina apenas os RRsets do tipo DNSKEY

Zone Signing Key (ZSK)

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

Conceito de Chaves

registro.br
Registro de Domínios para a Internet no Brasil

Key Signing Key (KSK)

As chaves utilizadas para assinar as chaves da zona, sendo, assina apenas os RRsets do tipo DNSKEY

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

Rollover (Substituição de Chaves - RFC 4641)

- Introduz um procedimento para mudanças periódicas das chaves KSK e ZSK
- Mantém a estrutura da zona e dos caches consistentes durante o período de mudança de chaves (aguarda os TTLs expirarem)

Cache

- Um cache DNS guarda localmente os resultados das requisições de resolução de nomes para utilização futura, evitando a repetição de pesquisas e aumentando drasticamente a velocidade de resposta
- O cache armazena as informações pelo período de tempo determinado no TTL (Tempo de Vida), que é um valor enviado junto a resposta de cada requisição

Rollover (Substituição de Chaves - RFC 4641)

TTL

- Quanto maior for seu TTL, mais tempo a determinada informação ficará armazenada em CACHE, sendo interessante apenas para servidores que atualizam pouco sua zona
- Quanto menor for seu TTL, maior será o tráfego de rede, pois os servidores recursivos irão frequentemente requisitar novos dados, sendo interessante apenas para servidores que atualizam sua zona frequentemente

Exemplos de valores para o TTL

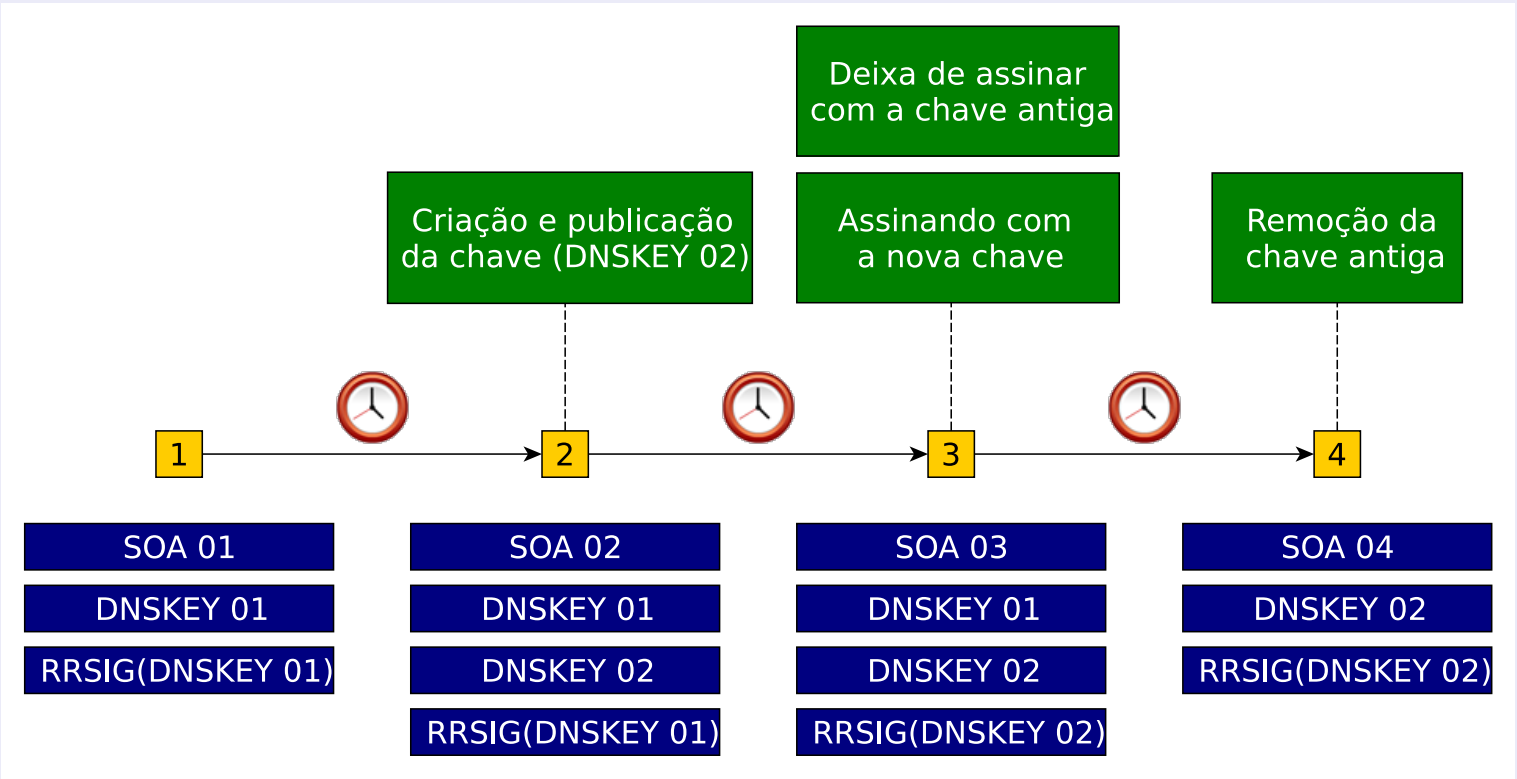
- 2 dias paras os records do APEX (possuem o nome da zona)
- 6 horas para a record DNSKEY
- 1 dia para os demais records

OBS: O record NSEC possuirá o TTL minimum determinado no record SOA (o record NSEC deve possuir um TTL baixo em razão do cache negativo)

OBS2: O record RRSIG possuirá o mesmo TTL do record que assinou

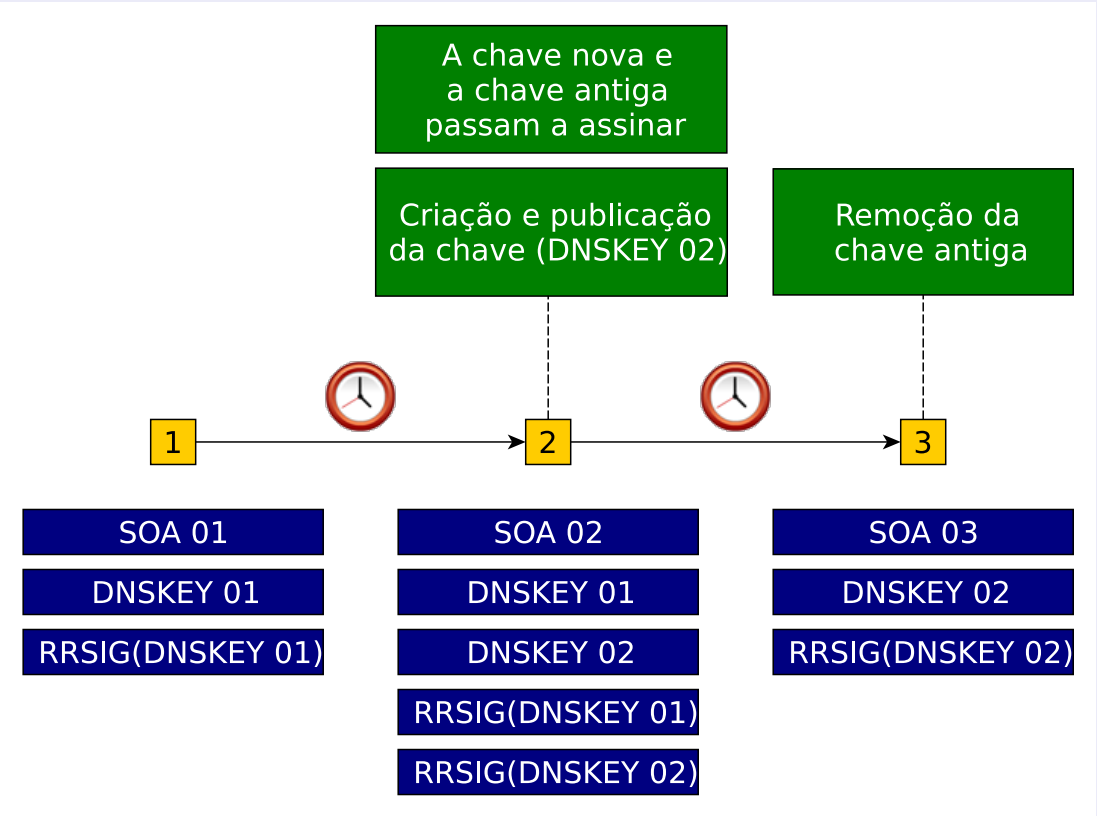
Rollover (Substituição de Chaves - RFC 4641)

Pre-Publish (utilizado na ZSK BR)



- 1 – 2 : A mudança da etapa 1 para a etapa 2 pode ser imediata
- 2 – 3 : Tempo de propagação para os servidores autoritativos + TTL do Key Set
- 3 – 4 : Tempo de propagação para os servidores autoritativos + TTL máximo da zona na versão antiga

Double Signing (utilizado na KSK BR)



- 1 – 2 : A mudança da etapa 1 para a etapa 2 pode ser imediata
- 2 – 3 : Tempo de propagação para os servidores autoritativos + TTL máximo da zona na versão antiga

Anúncios de Rollover do BR

Toda vez que ocorrer um processo de substituição da KSK da zona BR será enviado um aviso para as listas:

anuncios-dnssec	https://eng.registro.br/mailman/listinfo/anuncios-dnssec
GTER	https://eng.registro.br/mailman/listinfo/gter
GTS-L	https://eng.registro.br/mailman/listinfo/gts-l

Política de rollover da KSK BR utilizada pelo Registro.br

Substituições programadas da KSK BR são feitas uma vez ao ano. KSKs são válidas por 14 meses e é utilizada a técnica de double-signing. Durante um período de 2 meses existirão duas KSK BR ativas.

– Informações mais atualizadas podem ser encontradas em:

`https://registro.br/dnssec-policy.html`

Política de chaves utilizada pelo Registro.br

O Registro.br utiliza-se de 3 pares de chaves para assinatura em DNSSEC:

Política de chaves utilizada pelo Registro.br

O Registro.br utiliza-se de 3 pares de chaves para assinatura em DNSSEC:

1. **KSK BR:** Key Signing Key da zona BR. Sua chave privada é utilizada apenas para assinar o conjunto de chaves públicas da zona BR, ou seja, chaves públicas do KSK BR e ZSK BR.

Política de chaves utilizada pelo Registro.br

O Registro.br utiliza-se de 3 pares de chaves para assinatura em DNSSEC:

1. **KSK BR:** Key Signing Key da zona BR. Sua chave privada é utilizada apenas para assinar o conjunto de chaves públicas da zona BR, ou seja, chaves públicas do KSK BR e ZSK BR.
2. **ZSK BR:** Zone Signing Key da zona BR. Sua chave privada é utilizada para assinar registros da zona BR: conjunto de registros do apex da zona BR e conjunto de registros DS e NSEC.

Política de chaves utilizada pelo Registro.br

O Registro.br utiliza-se de 3 pares de chaves para assinatura em DNSSEC:

1. **KSK BR:** Key Signing Key da zona BR. Sua chave privada é utilizada apenas para assinar o conjunto de chaves públicas da zona BR, ou seja, chaves públicas do KSK BR e ZSK BR.
2. **ZSK BR:** Zone Signing Key da zona BR. Sua chave privada é utilizada para assinar registros da zona BR: conjunto de registros do apex da zona BR e conjunto de registros DS e NSEC.
3. **ZSK *.BR:** Zone Signing Key de algumas das zonas abaixo de BR. Sua chave privada é utilizada para assinar registros das zonas assinadas: conjunto de registros do apex destas zonas e conjunto de registros DS e NSEC.

Política de chaves utilizada pelo Registro.br

O Registro.br utiliza-se de 3 pares de chaves para assinatura em DNSSEC:

1. **KSK BR:** Key Signing Key da zona BR. Sua chave privada é utilizada apenas para assinar o conjunto de chaves públicas da zona BR, ou seja, chaves públicas do KSK BR e ZSK BR.
2. **ZSK BR:** Zone Signing Key da zona BR. Sua chave privada é utilizada para assinar registros da zona BR: conjunto de registros do apex da zona BR e conjunto de registros DS e NSEC.
3. **ZSK *.BR:** Zone Signing Key de algumas das zonas abaixo de BR. Sua chave privada é utilizada para assinar registros das zonas assinadas: conjunto de registros do apex destas zonas e conjunto de registros DS e NSEC.

Como o Registro.br tem autoridade sobre o BR e *.BR, não existe necessidade de KSK para *.BR.

Política de chaves utilizada pelo Registro.br

O Registro.br utiliza-se de 3 pares de chaves para assinatura em DNSSEC:

1. **KSK BR:** Key Signing Key da zona BR. Sua chave privada é utilizada apenas para assinar o conjunto de chaves públicas da zona BR, ou seja, chaves públicas do KSK BR e ZSK BR.
2. **ZSK BR:** Zone Signing Key da zona BR. Sua chave privada é utilizada para assinar registros da zona BR: conjunto de registros do apex da zona BR e conjunto de registros DS e NSEC.
3. **ZSK *.BR:** Zone Signing Key de algumas das zonas abaixo de BR. Sua chave privada é utilizada para assinar registros das zonas assinadas: conjunto de registros do apex destas zonas e conjunto de registros DS e NSEC.

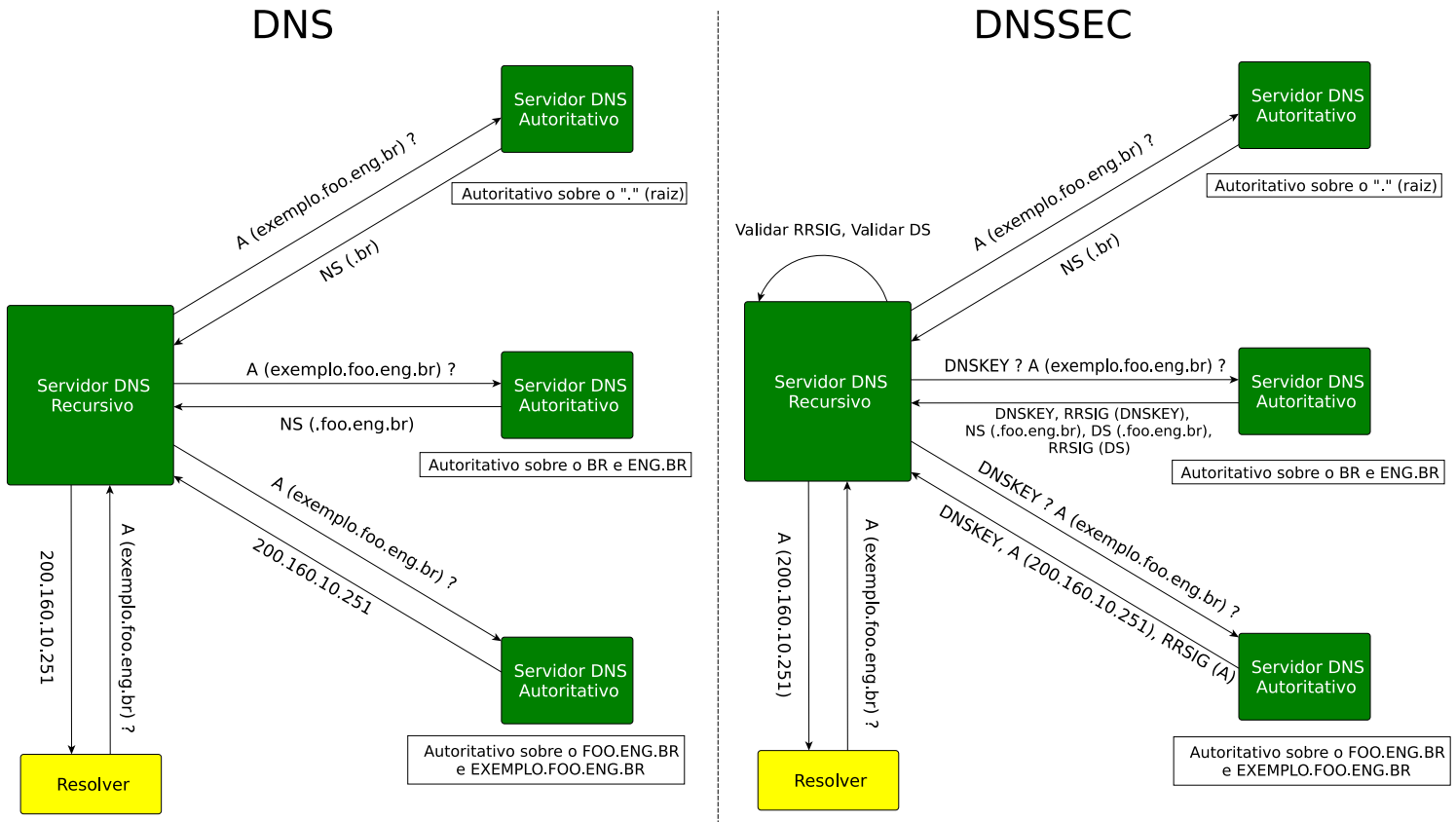
Como o Registro.br tem autoridade sobre o BR e *.BR, não existe necessidade de KSK para *.BR.

Validade das assinaturas

- Assinaturas geradas com KSKs BR têm validade de 4 meses.
- Assinaturas geradas com ZSKs têm validade de 7 dias.

DNS Vs DNSSEC

Diferenças entre uma requisição DNS e uma requisição DNSSEC:



8 Pacotes — X Bytes

12 Pacotes ± 6X Bytes[a]

[a] Diferença proporcional ao tamanho da chave

Parte II

Utilizando DNSSEC na Prática

Softwares

Compatibilidade DNSSEC

	Autoritativo	Recursivo	Caching	DNSSEC[a]	DNSSEC bis[b]	TSIG
ANS	√			√	√	√
BIND	√	√	√	√	√	√
CNS		√	√	√	√	√
djbdns	√	√	√			
IPControl	√	√	√	√	√	√
IPM DNS	√	√	√	√	√	√
MaraDNS	√	√	√			
NSD	√			√	√	√
PowerDNS	√	√	√			
Microsoft DNS	√	√	√	√		√
VitalQIP	√	√	√	√	√	?

[a] Versão antiga do protocolo não suportada pelo Registro.br

[b] Versão atual do protocolo

Softwares

Compatibilidade de Servidores DNS com Sistemas Operacionais

	BSD	Solaris	Linux	Windows	MAC OS X
ANS	√	√	√	?	?
BIND	√	√	√	√	√
CNS	√	√	√	?	?
djbdns	√	√	√		√
IPControl		√	√	√	
IPM DNS	√	√	√		√
MaraDNS	√	√	√	√[a]	√
NSD	√	√	√	?	√
PowerDNS	√	√	√	√	√[b]
Microsoft DNS				√	
VitalQIP		√	√	√	

[a] Apenas nas versões mais recentes do sistema operacional

[b] Software em versão Beta

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

DIG (Domain Information Groper)

Uma ferramenta para consultas sobre registros DNS

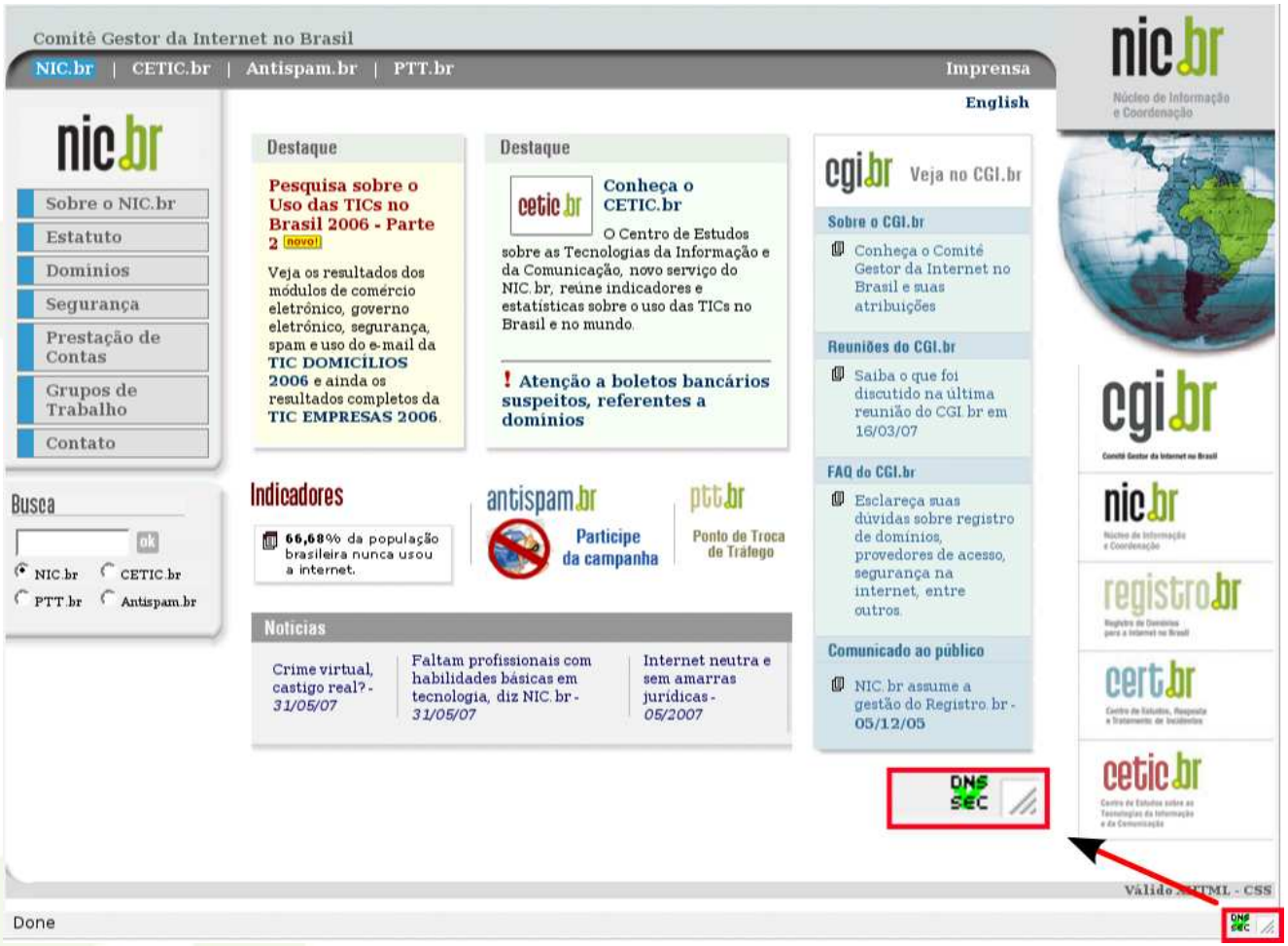
– para validação da cadeia de confiança é necessário compilar com a opção **sigchase** habilitada

DRILL

Uma ferramenta similar ao DIG com suporte nativo a DNSSEC

Plugin para o navegador Firefox que permite validar a cadeia de confiança caso o domínio esteja com DNSSEC habilitado

– http://www.nlnetlabs.nl/dnssec/drill_extension.html



Após instalar o plugin, altere em suas configurações a localização das "trusted-keys"em seu computador.

No diretório das "trusted-keys", cada arquivo existente (o nome é indiferente) deve possuir uma chave no seguinte formato:

```
br.  IN DNSKEY 257 3 5
AwEAAcmqkFULGgm1VlBbUYQEuCzSbEByjAcNInY9gxftbTK+CSYwlGAfxl5hwx7kxOQAZ2ZMLrxD+sTQVC4StoAPPcUhFqEGOV+9G
I6SsD/fikQ0IhtXaS6INKkOPOkfBqotk6C5QbbVXcsML54/dtZYWi/Z7CaG2Hz93ouyUMQzIPohER+gkbFYq3ewDajqJKNsVm8caT
9/mkNw+CQHR+QNmWM=
```

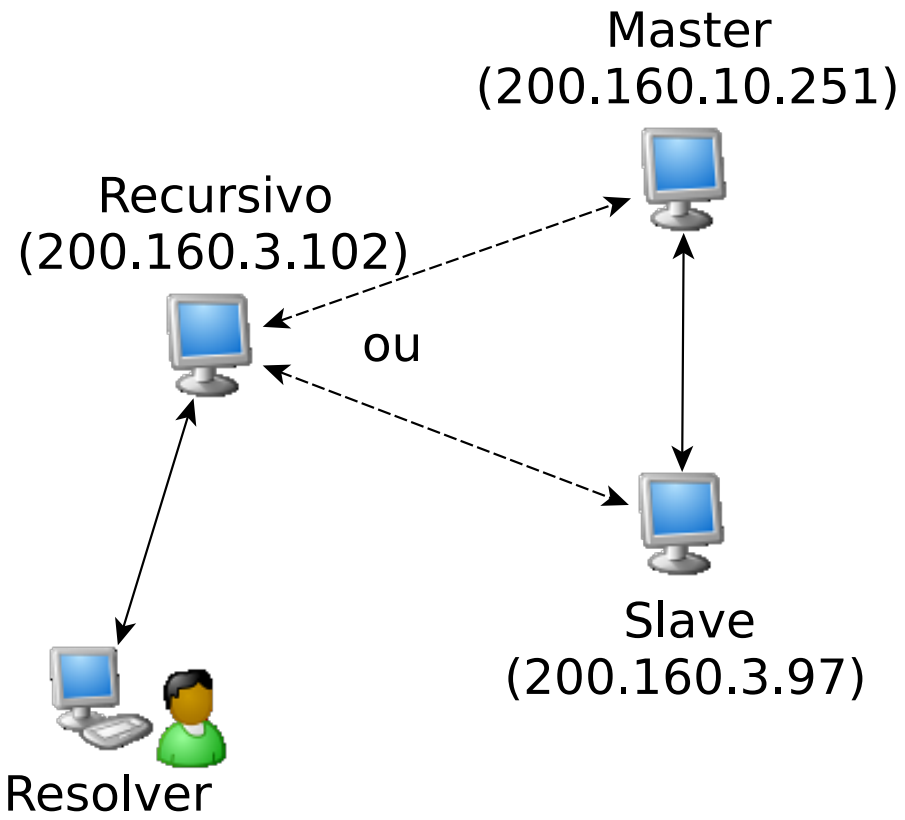
Demonstração prática

registro.br
Registro de Domínios para a Internet no Brasil

1. Configuração BIND
   a. Arquivo de zona
   b. named.conf
2. Teste – Consulta de Record
3. Registro de domínio – atualização dos nameservers
4. Aguardar nova publicação
5. Configuração DNSSEC no BIND
   a. Geração da chave ZSK
   b. Geração da chave KSK
   c. Atualização do arquivo de zona
   d. Assinatura da zona
   e. Atualização do named.conf
6. Teste – Consulta de Record com DNSSEC
7. Atualização do Record DS no cadastro do domínio
8. Aguardando nova publicação
9. Teste – Validação da cadeia de confiança

nic.br

Ambiente de Testes



Arquivo de Zona

Arquivo db.foo

```
foo.eng.br. IN SOA ns1.foo.eng.br. hostmaster.foo.eng.br. (
            1       ; serial
            3600    ; refresh
            3600    ; retry
            3600    ; expire
            900 )   ; minimum TTL
foo.eng.br. IN NS ns1.foo.eng.br.
foo.eng.br. IN NS ns2.foo.eng.br.
exemplo.foo.eng.br. IN NS ns2.exemplo.foo.eng.br.
exemplo.foo.eng.br. IN NS ns1.exemplo.foo.eng.br.
ns1.foo.eng.br. IN A 200.160.3.97
ns2.foo.eng.br. IN A 200.160.10.251
ns1.exemplo.foo.eng.br. IN A 200.160.3.97
ns2.exemplo.foo.eng.br. IN A 200.160.10.251
```

Arquivo db.exemplo.foo

```
exemplo.foo.eng.br. IN SOA ns.exemplo.foo.eng.br. hostmaster.exemplo.foo.eng.br. (
                    1       ; serial
                    3600    ; refresh
                    3600    ; retry
                    3600    ; expire
                    900 )   ; minimum TTL
exemplo.foo.eng.br. IN NS ns1.exemplo.foo.eng.br.
exemplo.foo.eng.br. IN NS ns2.exemplo.foo.eng.br.
ns1.exemplo.foo.eng.br. IN A 200.160.3.97
ns2.exemplo.foo.eng.br. IN A 200.160.10.251
```

named.conf (master)

```
options {
    directory "/etc/namedb";
    pid-file "/var/run/named/pid";
    dump-file "/var/dump/named_dump.db";
    statistics-file "/var/stats/named.stats";
    listen-on { 200.160.10.251; };
};
zone "foo.eng.br" {
    type master;
    file "/etc/namedb/db.foo";
    allow-transfer {
        200.160.3.97;
    };
};
zone "exemplo.foo.eng.br" {
    type master;
    file "/etc/namedb/db.exemplo.foo";
    allow-transfer {
        200.160.3.97;
    };
};
```

named.conf (slave)

```
options {
    directory "/etc/namedb";
    pid-file "/var/run/named/pid";
    dump-file "/var/dump/named_dump.db";
    statistics-file "/var/stats/named.stats";
    listen-on { 200.160.3.97; };
};
zone "foo.eng.br" {
    type slave;
    file "/etc/namedb/db.foo";
    masters {
        200.160.10.251;
    };
};
zone "exemplo.foo.eng.br" {
    type slave;
    file "/etc/namedb/db.exemplo.foo";
    masters {
        200.160.10.251;
    };
};
```

Teste - Consulta de record

Zona foo.eng.br

dig @200.160.10.251 foo.eng.br soa +noadditional +multiline

```
; <<>> DiG 9.3.3 <<>> @200.160.10.251 foo.eng.br soa +noadditional +multiline
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40573
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
;; QUESTION SECTION:
;foo.eng.br.                IN SOA
;; ANSWER SECTION:
foo.eng.br.                900 IN SOA ns1.foo.eng.br. hostmaster.foo.eng.br. (
                                      1          ; serial
                                      3600       ; refresh (1 hour)
                                      3600       ; retry (1 hour)
                                      3600       ; expire (1 hour)
                                      900        ; minimum TTL (15 minutes)
                                      )
;; AUTHORITY SECTION:
foo.eng.br.                900 IN NS ns1.foo.eng.br.
foo.eng.br.                900 IN NS ns2.foo.eng.br.
;; Query time: 1 msec
;; SERVER: 200.160.10.251#53(200.160.10.251)
;; WHEN: Wed May 23 16:05:56 2007
;; MSG SIZE  rcvd: 143
```

Teste - Consulta de record

registro.br
Registro de Domínios para a Internet no Brasil

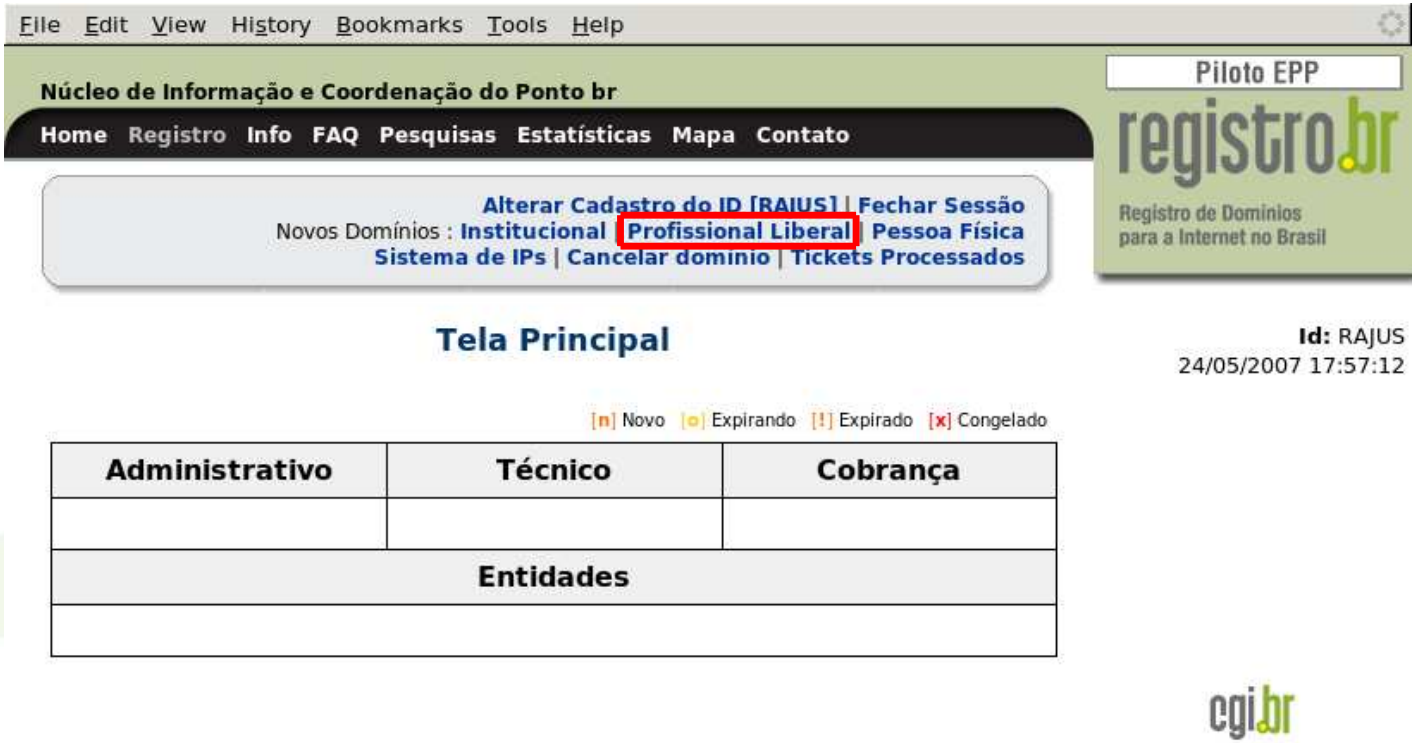
Zona exemplo.foo.eng.br

dig @200.160.10.251 exemplo.foo.eng.br soa +noadditional +multiline

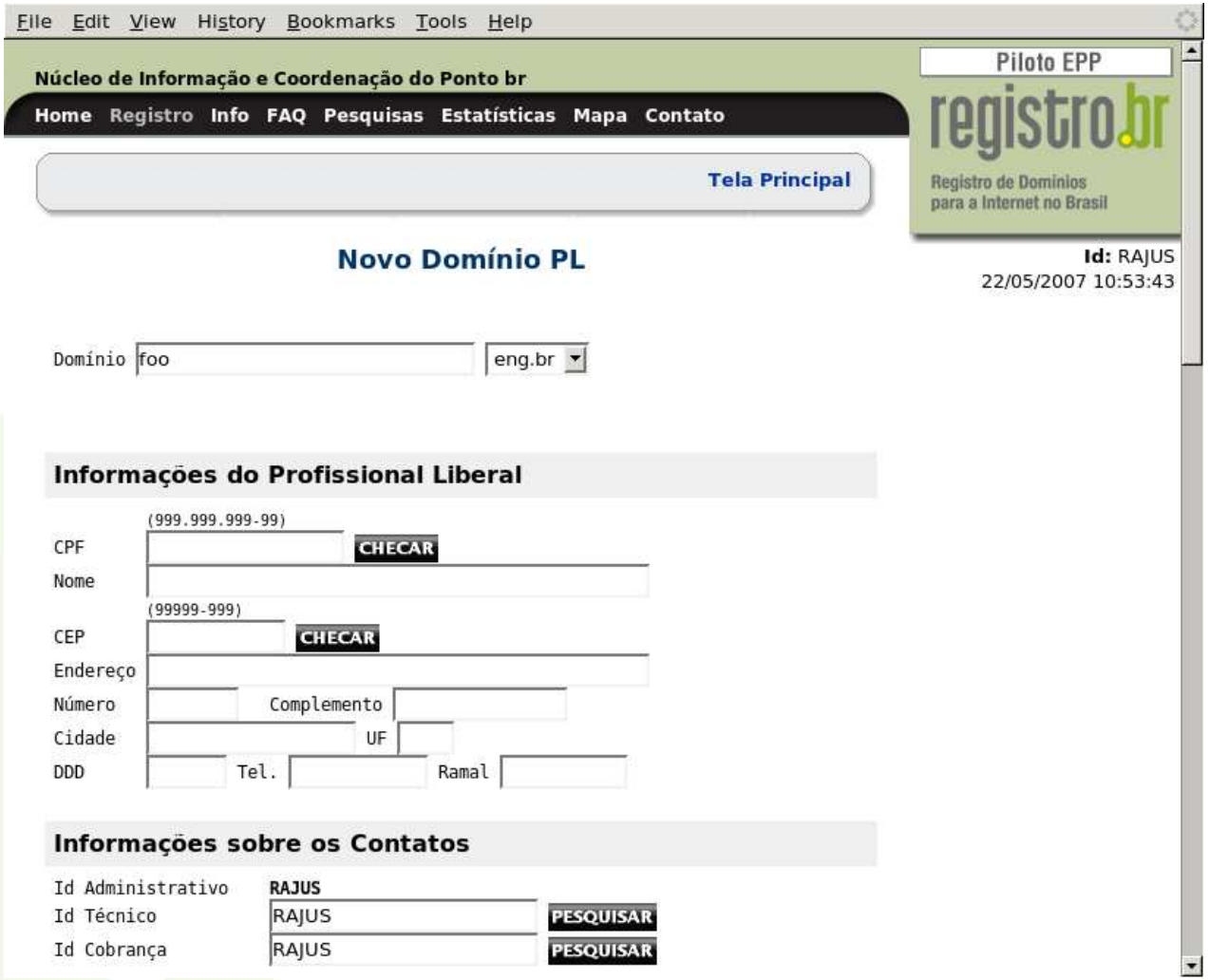
```
; <<>> DiG 9.3.3 <<>> @200.160.10.251 exemplo.foo.eng.br soa +noadditional +multiline
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63826
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
;; QUESTION SECTION:
;exemplo.foo.eng.br.     IN SOA
;; ANSWER SECTION:
exemplo.foo.eng.br.     900 IN SOA ns.exemplo.foo.eng.br. hostmaster.exemplo.foo.eng.br. (
                                1           ; serial
                                3600        ; refresh (1 hour)
                                3600        ; retry (1 hour)
                                3600        ; expire (1 hour)
                                900         ; minimum TTL (15 minutes)
                                )
;; AUTHORITY SECTION:
exemplo.foo.eng.br.     900 IN NS ns2.exemplo.foo.eng.br.
exemplo.foo.eng.br.     900 IN NS ns1.exemplo.foo.eng.br.
;; Query time: 2 msec
;; SERVER: 200.160.10.251#53(200.160.10.251)
;; WHEN: Wed May 23 16:10:58 2007
;; MSG SIZE  rcvd: 154
```

nic.br

Registro de domínios na Beta

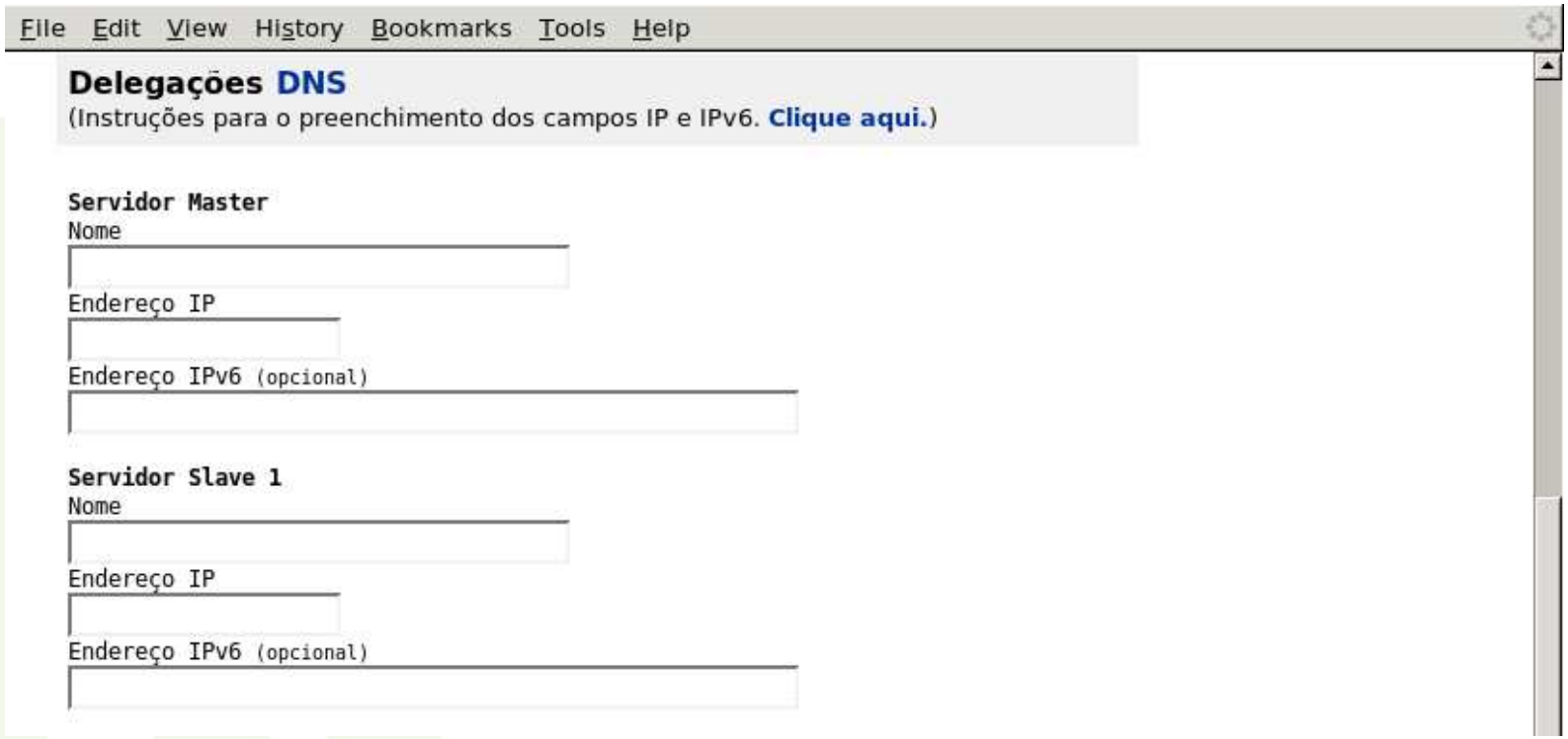


Registro de domínios na Beta



Registro de domínio na Beta

Delegações DNS



Aguardando nova publicação

registro.br
Registro de Domínios para a Internet no Brasil

Após estes procedimentos é necessário aguardar uma nova publicação

nic.br

Geração da chave KSK

BIND: dnssec-keygen

Zona foo.eng.br:

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

Zona exemplo.foo.eng.br:

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

Onde,

- -f : Define o tipo da chave
- -a : Algoritmo
- -b : Tamanho da chave (bytes)
- -n : Especifica o tipo de dono da chave

OBS: Guardar o nome das chaves geradas relacionando qual é KSK e qual é ZSK para ser usado futuramente.
OBS2: Chaves geradas com dnssec-keygen não possuem passphrase.

Tamanho das chaves

- KSK BR: 1280 bits

Geração da chave ZSK

BIND: dnssec-keygen

Zona foo.eng.br:

```
dnssec-keygen -a RSASHA1 -b 1024 -n ZONE foo.eng.br
```

Zona exemplo.foo.eng.br:

```
dnssec-keygen -a RSASHA1 -b 1024 -n ZONE exemplo.foo.eng.br
```

Onde,

- -a : Algoritmo
- -b : Tamanho da chave (bytes)
- -n : Tipo de chave

OBS: Guardar o nome das chaves geradas relacionando qual é KSK e qual é ZSK para ser usado futuramente.
OBS2: Chaves geradas com dnssec-keygen não possuem passphrase.

Tamanho das chaves

- KSK BR: 1280 bits
- ZSK BR: 1152 bits
- ZSK *.BR: 1024 bits

Inclusão das chaves no arquivo de zona

Arquivo db.foo

```
foo.eng.br. IN SOA ns1.foo.eng.br. hostmaster.foo.eng.br. (
            2         ; serial
            3600      ; refresh
            3600      ; retry
            3600      ; expire
            900 )     ; minimum TTL
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 200.160.10.251
ns1.exemplo.foo.eng.br. IN A 200.160.3.97
ns2.exemplo.foo.eng.br. IN A 200.160.10.251
$include Kfoo.eng.br.+005+62745.key
$include Kfoo.eng.br.+005+00817.key
```

OBS

O serial deve ser incrementado todas as vezes em que o arquivo de zona for modificado

Inclusão das chaves no arquivo de zona

registro.br
Registro de Domínios para a Internet no Brasil

Arquivo db.exemplo.foo

```
exemplo.foo.eng.br. IN SOA ns.exemplo.foo.eng.br.
hostmaster.exemplo.foo.eng.br. (
                    2       ; serial
                    3600    ; refresh
                    3600    ; retry
                    3600    ; expire
                    900 )   ; minimum TTL
exemplo.foo.eng.br. IN NS ns1.exemplo.foo.eng.br.
exemplo.foo.eng.br. IN NS ns2.exemplo.foo.eng.br.
ns1.exemplo.foo.eng.br. IN A 200.160.3.97
ns2.exemplo.foo.eng.br. IN A 200.160.10.251
$include Kexemplo.foo.eng.br.+005+11970.key
$include Kexemplo.foo.eng.br.+005+03112.key
```

OBS

O serial deve ser incrementado todas as vezes em que o arquivo de zona for modificado

Assinar as zonas

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 -o foo.eng.br db.foo
```

Zona exemplo.foo.eng.br:

```
$ dnssec-signzone -o exemplo.foo.eng.br db.exemplo.foo
```

Onde,

- -o : Nome da zona
- 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 sera utilizado para as delegações.
– o arquivo gerado neste exemplo: `dsset-foo.eng.br.`

Inclusão do DS da delegação

O DS contido no arquivo dsset-exemplo.foo.eng.br. deverá ser adicionado no arquivo db.foo.signed de forma a continuar a cadeia de confiança entre o domínio (foo.eng.br) e suas delegações (exemplo.foo.eng.br)

```
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 TTL (15 minutes)
                )
            RRSIG SOA 5 3 900 20070629103957 (
                20070530103957 62745 foo.eng.br.
                uLVZ42puk3vYcfaPg8c7jKl8BeyTU/HEuupJ643g6aJB
                27s8eP8LndVPOt/XnPk8l3R+FNdaKgirmI3XZJrSn92r
                Q1z3oh8rYkmwqs9JZyeQFL73xyjT1+6uikyK3fprAM1R
                JcyBL9ECK/65BDivgrfqQ7HUARYwsW0b7NtOrb0= )
            NS ns1.foo.eng.br.
            NS ns2.foo.eng.br.
            ...
            exemplo.foo.eng.br.     IN DS 3112 5 1 386B4390C5B30DB65D74EA8B660978077171948C
```

Atualização do named.conf

Necessário atualizar no Master e no Slave

Habilitar a opção de DNSSEC

```
options {
    directory "/etc/namedb";
    pid-file "/var/run/named/pid";
    dump-file "/var/dump/named_dump.db";
    statistics-file "/var/stats/named.stats";
    dnssec-enable yes;
    listen-on { 200.160.3.97; };
};
```

Atualização do named.conf

Necessário atualizar no Master

Alteração da referência para o arquivo de zona

```
zone "foo.eng.br" {
    type master;
    file "/etc/namedb/db.foo.signed";
    allow-transfer {
        200.160.3.97;
    };
};
zone "exemplo.foo.eng.br" {
    type master;
    file "/etc/namedb/db.exemplo.foo.signed";
    allow-transfer {
        200.160.3.97;
    };
};
```

Ancorando a KSK da Zona ".br" (Recursivo)

registro.br
Registro de Domínios para a Internet no Brasil

Obtendo a KSK a ser ancorada

- .BR `https://registro.br/ksk/`
- DLV `https://secure.isc.org/index.pl?/ops/dlv/index.php`

1. Instalar o BIND, mantendo as configurações padrão
2. No arquivo named.conf, definir "dnssec-enable yes" nas opções
3. Obtenha a chave pública KSK da zona br
4. Inserir a chave pública no bloco denominado "trusted-keys" no arquivo named.conf

nic.br

Ancorando a KSK da Zona ".br" (Recursivo)

registro.br
Registro de Domínios para a Internet no Brasil

Exemplo de inclusão de uma "Trusted Key"

```
options {
    directory "/etc/namedb";
    pid-file "/var/run/named/pid";
    dump-file "/var/dump/named_dump.db";
    statistics-file "/var/stats/named.stats";
    dnssec-enable yes;
    dnssec-validation yes;
    listen-on { 200.160.3.102; };
};
trusted-keys {
br.                     257 3 5
                        "AwEAAa290pX9aaNf053wZdkOGKmNCbLlbyCo1yNrwDiv
                        fgyBcdT+cjtVwSEmzh6HoY+lQeJKJDpbJF1/G9ZbA/Aw
                        rKCpahLFDz5SaZiP0sStuWg8UzWz8b5J5t2dlxsu6PeF
                        dU08fkItt1FDEGCxsy3IR+eYJGdK0jowuDySoiQ8Uj/+
                        3ZHM4I4z2gOzEwb8uI3Jntmj5azop4B2o1WDNV1VdPJl
                        96TvMy5ImGsBkn03y3FUrQpynQn8M2x5pztuGEOg8KPZ
                        Yp/VUp0V0HyqTjSPsM+mCT2x80xN5SghaMeby85u5fVs
                        OEks3T6fN27nFxrdnMvcmNlslwcQvbxWSwTNVeU=";
};

...
```

nic.br

Teste - Consulta de record com DNSSEC

registro.br
Registro de Domínios para a Internet no Brasil

Zona foo.eng.br

dig @200.160.10.251 foo.eng.br soa +dnssec +noadditional +multiline

```
;; ANSWER SECTION:
foo.eng.br.             900 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 TTL (15 minutes)
                                )
foo.eng.br.             900 IN RRSIG SOA 5 3 900 20070617200428 (
                                20070518200428 62745 foo.eng.br.
                                glEeCYyd/CCBfzH64y0RAQf9OxYDsI4xuBNaam+8DZQZ
                                xeoSLQEEtwmp6wBtQ7G10wSM9nEjRRhbZdNPNKJMp2PE
                                lLLgLI+BLwdlzOt8MypcpLOaTm9rc7pP7UR5XLzU1k8D
                                m6ePW1bNkId7i0IPSghyoHM7tPVdL2GW51hCujA= )
;; 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+UeqYk0xgQGQQXkBzcKiKQRPwe+1JZlpjEzj
                                U1Uj0HUOHefajXzMv7FlFMWYeU51Ybg49HFe67XQVlK5
                                4GeAFXWB7YS59yODLoNEBxQl9QEy6g/OOnLpuKTrST8q
                                qd5Fc/eYqN/Ag3GnfcAviZgiQhhveGH9mJHWZyc= )
```

nic.br

Teste - Consulta de record com DNSSEC

registro.br
Registro de Domínios para a Internet no Brasil

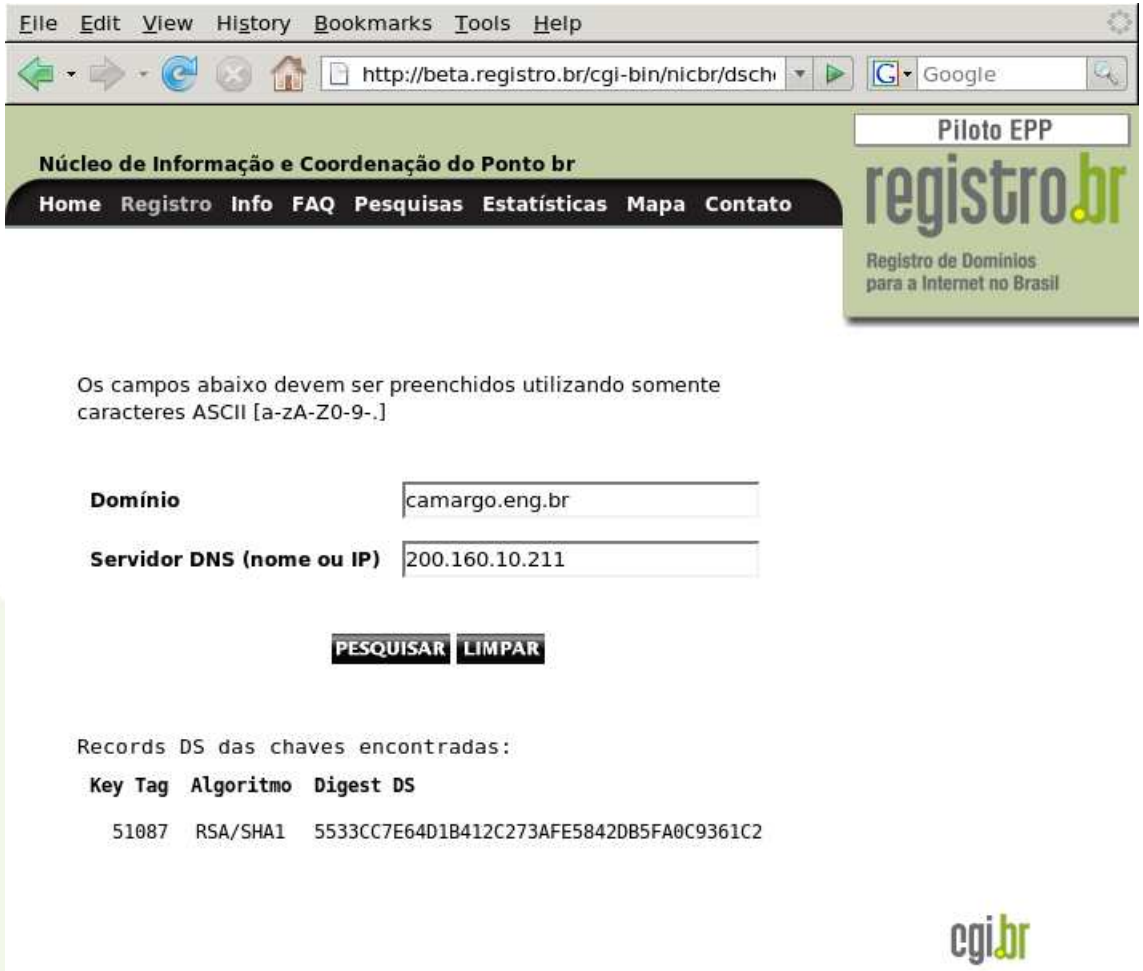
Zona exemplo.foo.eng.br

dig @200.160.10.251 exemplo.foo.eng.br soa +dnssec +noadditional +multiline

```
;; ANSWER SECTION:
exemplo.foo.eng.br.      900 IN SOA ns.exemplo.foo.eng.br. hostmaster.exemplo.foo.eng.br. (
                                 2          ; serial
                                 3600       ; refresh (1 hour)
                                 3600       ; retry (1 hour)
                                 3600       ; expire (1 hour)
                                 900        ; minimum TTL (15 minutes)
                                 )
exemplo.foo.eng.br.      900 IN RRSIG SOA 5 4 900 20070617184743 (
                                 20070518184743 11970 exemplo.foo.eng.br.
                                 QAPzSENr7i17xRkJ6vL1BunpSzDoVY+naCOwv9kRUB9s
                                 yPqKx3RrKi/+u0sJYAUG3CDjFzggQ93yu7VFg6oIb0lD
                                 cFV22vYbz5/ykx+LOHrgyszItPRH4CfOSbQG1wXczPr2
                                 FmeYj5AlwdcjqkTLCf0Ef/oOylnp6x+2F/BSKiU= )
;; AUTHORITY SECTION:
exemplo.foo.eng.br.      900 IN NS ns1.exemplo.foo.eng.br.
exemplo.foo.eng.br.      900 IN NS ns2.exemplo.foo.eng.br.
exemplo.foo.eng.br.      900 IN RRSIG NS 5 4 900 20070617184743 (
                                 20070518184743 11970 exemplo.foo.eng.br.
                                 t7a3FEqAIW/roFQERDYyR+V6qT17erabiAtsLgOJQkw3
                                 AEBQ9tS1dvdpZq29uIn2cpqbuLj+DNPagubHO+C+tiTQ
                                 o3IZj+sb8DNWb2zrTuoOYT96eCehX20Dq4tLliHpCcyq
                                 UANY/+KkJp+yAXgVRzByIfXFFHZwqysUYr+WI+I= )
```

nic.br

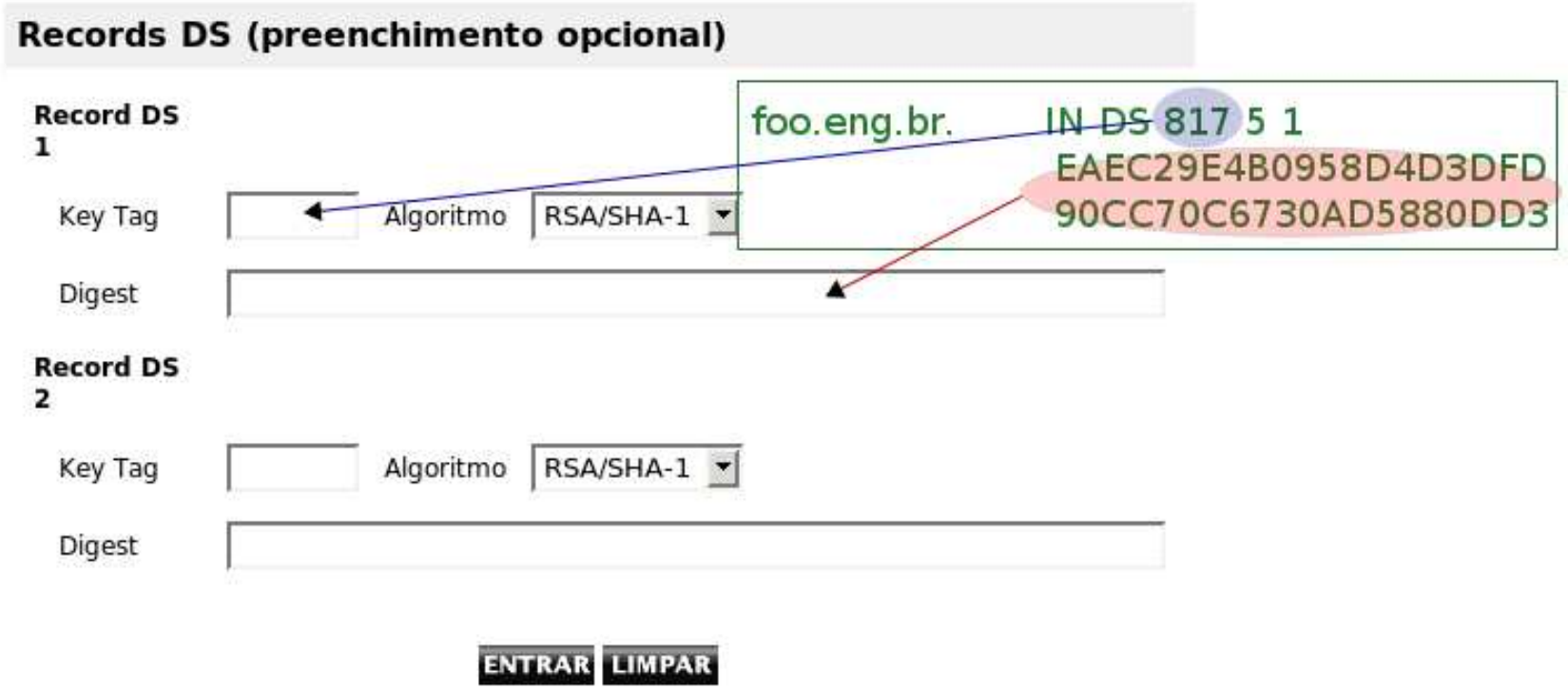
DS Check



- Calcula o record DS a partir da DNSKEY
- Útil para validar um DS gerado por software de terceiros

Atualização do registro de domínios incluindo o DS

Apartir do arquivo `dsset-foo.eng.br.`



O número após o `Key Tag` no Record se refere ao `Algoritmo` (RFC 4034 - A.1)

- 3 DSA
- 5 RSA

O número antes do `Digest` no Record se refere ao `Digest Type` (RFC 4034 - A.1)

- 1 SHA-1

Aguardando nova publicação

registro.br
Registro de Domínios para a Internet no Brasil

Após estes procedimentos é necessário aguardar uma nova publicação

nic.br

Teste - Validação da cadeia de confiança

registro.br
Registro de Domínios para a Internet no Brasil

DIG - Sigchase

- O sigchase é uma opção no DIG que permite realizar uma verificação em toda a estrutura desde o ponto assinado até o domínio fornecido
- Útil na verificação da validade nas assinaturas e chaves das zonas
- Para utilizar DIG +sigchase, é necessário compilar o BIND 9.4 com a variável de ambiente "`STD_CDEFINES`" definida com o valor "`-DDIG_SIGCHASE=1`"

Ancorando chave para o DIG +sigchase

1. Obter a chave pública da ZSK da "`.br`" fornecida pelo Registro.br
2. Copiar a chave no arquivo `/etc/trusted-key.key`
   não deixar nenhuma quebra de linha dentro da chave
   não deixar nenhuma linha em branco após a chave

nic.br

Teste - Validação da cadeia de confiança

registro.br
Registro de Domínios para a Internet no Brasil

Exemplo

dig @200.160.3.69 exemplo.foo.eng.br soa +sigchase +multiline

```
;; RRset to chase:
eng.br.                 172800 IN SOA a.dns.br. hostmaster.registro.br. (
                                2007033785 ; serial
                                1800       ; refresh (30 minutes)
                                900        ; retry (15 minutes)
                                604800     ; expire (1 week)
                                900        ; minimum TTL (15 minutes)
                                )
;; RRSIG of the RRset to chase:
eng.br.                 172800 IN RRSIG SOA 5 2 172800 20070531204953 (
                                20070528174953 32986 eng.br.
                                ED6Xp/67/i6n7XhjEA4AmzmoWAPWgJLescK9UIu2bkqH
                                RKJS/gDa9voLjfDHnwnjHViq6aXt2AIi4Zj5T/I+5+mB
                                BDWEnuOpG9a4A7v4jAUIT78c5jlkRh2BvLw4QZdiEbuH
                                253Yq1xRUZCta37Qm4IKRgN40osNMRtfBy/BuXY= )
Launch a query to find a RRset of type DNSKEY for zone: eng.br.
;; DNSKEYset that signs the RRset to chase:
eng.br.                 21600 IN DNSKEY 257 3 5 (
                                AwEAAbAgpvVTb3Pn7Oj7JDvfCZQLtyRDoJdo6G2mBeuM
                                fZXXx+Cj0qIhkmZZlzDTh3KyJ1Rbl1WuD6+EEXey4LQm
                                qET3B7yUqrOCeSfCzHeeYYzYNRgIhKvinbWqJ2le5SMg
                                HxbASmezNm/rQmQHkYqLaDt9zw/rrwMSVyeh5DEEQc/P
                                ) ; key id = 32986
```

nic.br

registro.br
Registro de Domínios para a Internet no Brasil

Exemplo (Continuação)

```
;; RRSIG of the DNSKEYset that signs the RRset to chase:
eng.br.                 21600 IN RRSIG DNSKEY 5 2 21600 20070531204953 (
                                20070528174953 32986 eng.br.
                                nVf9AmuMrMWLpWl0R6I38pjXRkaE/9bYJrdvEAbSLPDD
                                7kVyHexcis79EGp/GUgwG6/0towLvzW1y8PfqcbbgQhK
                                5hjyH+ngKwBQUkGAjVw3Ysgi9kJcKAfU042zhIe//xSY
                                y3w+j87FmA67nwVyCqtz+cwmWPvsuqe6OQwNlD8= )
Launch a query to find a RRset of type DS for zone: eng.br.
;; DSset of the DNSKEYset
eng.br.                 86400 IN DS 32986 5 1 (
                                6E4CF7F759FDFE1F08E658AC505BC53BFD07915E )
;; RRSIG of the DSset of the DNSKEYset
eng.br.                 86400 IN RRSIG DS 5 2 86400 20070531204953 (
                                20070528174953 60165 br.
                                eT6fMTSGksBuagswjDfBI/YAegN+s6Xmfb3Awwe1AgrS
                                dUFOvlcLU6pkvwgFROfDnjb7oU1kW2p3S5vEVuEu3LN8
                                lYfswjmW7MMw68X44jY1xtsYkC5sO0exxksrGCIrg+Vi
                                Ah7fMy1EIIybaAjqILq/iOOpqqeenJXjpI7iHVI= )
```

nic.br

Teste - Validação da cadeia de confiança

registro.br
Registro de Domínios para a Internet no Brasil

Exemplo (Continuação)

```
;; WE HAVE MATERIAL, WE NOW DO VALIDATION
;; VERIFYING SOA RRset for eng.br. with DNSKEY:32986: success
;; OK We found DNSKEY (or more) to validate the RRset
;; Now, we are going to validate this DNSKEY by the DS
;; OK a DS valids a DNSKEY in the RRset
;; Now verify that this DNSKEY validates the DNSKEY RRset
;; VERIFYING DNSKEY RRset for eng.br. with DNSKEY:32986: success
;; OK this DNSKEY (validated by the DS) validates the RRset of the DNSKEYs, thus the DNSKEY validates the
RRset
;; Now, we want to validate the DS :  recursive call
Launch a query to find a RRset of type DNSKEY for zone: br.
;; DNSKEYset that signs the RRset to chase:
br.                     21600 IN DNSKEY 257 3 5 (
                              AwEAAaeACjj1oWq1bzK3eFIHyqKCMrJ+cCKbBpJ2X8Dx
                              nu8PknEbsxgJaSXT5SeUphXGCTMgxYbwu6fefA7cS1OO
                              zfkG9Mq3HMaxXgKCZdhy+GOL9xVFTDOhZm+8dUNG2LQG
                              YCeqghu86lSZGSoB6gCG5HN3p1R7K8gKSqj8JGsRplQu
                              hPye+WGey1Cnm5gm+gHz/3JzlGAOmf3DSU8hI9j88tnp
                              hMRqUpRbEJPZQYD01EJl9CCRF0/kKnZyYgB8gh1IHrl0
                              vRIhxN77ztjJi7PWgk6Jq/pL4eH6hcHwIs2JPR3m+ptS
                              nav7UlMt2kiFD4IN2rcdD+eovWLAvzpvzeThC8M=
                              ) ; key id = 1657
                        21600 IN DNSKEY 256 3 5 (
                              AwEAAeHOt8VKghhsM1W1ps0XLkS4xrYVfPUvxO3av2tI
                              sTSdxr5j23C+Zs4AwdxAO6WkiUs3ik8oI3kBTNq5fUVf
                              jZkpoCkfGmxiwi0oT3jejVRDHQeriCVRZAbrY2JnAkVq
                              2+c1ajc1Hr6/knOz6hzv9p5JpLdfa454jBT7jH681j7L
                              ) ; key id = 60165
```

registro.br
Registro de Domínios para a Internet no Brasil

Exemplo (Continuação)

```
;; RRSIG of the DNSKEYset that signs the RRset to chase:
br.                     3600 IN RRSIG DNSKEY 5 1 21600 20070531204953 (
                                20070528174953 60165 br.
                                uF1LQOCYses5zHaOZe33zwd6j1Kkkm74NJ6hyWky16Ic
                                TEZiJKucbHd9U+8K6zUxskrA77Vx6rODOu7cmUSnxjDz
                                uPr2f2VJcTAW5nHrEk3u/8DU3gkyYdAIYu22KvGo+s4i
                                dEWssbiXOOQjvABDDXV3UyAJsNkakvIHAjOiEyA= )
                        3600 IN RRSIG DNSKEY 5 1 3600 20080101120000 (
                                20070101000000 1657 br.
                                flkMiXop002+y1j5gxsbKFXgi1pB90t2Fmj7oXuJ5vBE
                                eb+1vy+qV03GbR29FIrMKbX7fWT7qCVISSN87bDNr/UJ
                                4hNRZ57q8tmX1S/1oSJjhqHcWYAguRFApiRsywLKUtws
                                ZpkEW69BNWVu4UVVqPIJdwlCcNyy2MDVVKjzwXGaAp/Q
                                H2D+LMOsPpnRQFJua3rhynatsySJLvo1j3lw16oV1xDc
                                q7wAMTvkLtck8LRfNy6SWEvC4m++uPdwWPLZvSMBGMYh
                                wMY91/1eVz7sWQ+ThCcpLt17niCdSiqyMIPcziOjlBOm
                                jD/DOOzSscqp3UNdILCIqGo2mBjgLeARxQ== )
Launch a query to find a RRset of type DS for zone: br.
;; NO ANSWERS: no more
;; WARNING There is no DS for the zone: br.
;; WE HAVE MATERIAL, WE NOW DO VALIDATION
;; VERIFYING DS RRset for eng.br. with DNSKEY:60165: success
;; OK We found DNSKEY (or more) to validate the RRset
;; Ok, find a Trusted Key in the DNSKEY RRset: 1657
;; VERIFYING DNSKEY RRset for br. with DNSKEY:1657: success
;; Ok this DNSKEY is a Trusted Key, DNSSEC validation is ok: SUCCESS
```

nic.br

Roteiro - Assinar uma Zona

registro.br
Registro de Domínios para a Internet no Brasil

1. Verificar a disponibilidade do domínio junto ao registro.br
2. Instalar BIND
3. Configurar um arquivo de zona no servidor Master
4. Configurar o arquivo named.conf no servidor Master
5. Configurar o arquivo named.conf no servidor Slave
6. Executar o BIND (named) no servidor Master
7. Executar o BIND (named) no servidor Slave
8. Registrar o domínio no Registro.br
9. Aguardar nova publicação
10. Realizar testes no servidor (DIG)

11. Criar chave KSK (dnssec-keygen)
12. Criar chave ZSK (dnssec-keygen)
13. Incluir as chaves geradas no arquivo de zona do servidor Master
14. Assinar a zona (dnssec-signzone)
15. Incluir no arquivo de zona assinado (.signed) o DS de cada delegação assinada
16. Atualizar o named.conf do servidor Master de forma a utilizar o arquivo de zona .signed e habilitar DNSSEC-ENABLE
17. Atualizar o named.conf do servidor Slave habilitando DNSSEC-ENABLE
18. Restartar o BIND (named) no servidor Master
19. Restartar o BIND (named) no servidor Slave
20. Adicionar na interface de provisionamento o DS (localizado no arquivo dsset*)
21. Aguardar nova publicação

nic.br

Roteiro - Configurar um Servidor Recursivo

1. Instalar biblioteca de desenvolvimento do OpenSSL
2. Instalar BIND com sigchase
3. Configurar o arquivo named.conf habilitando DNSSEC-ENABLE e DNSSEC-VALIDATION
4. Obter a trusted-key do site do Registro.br
5. Incluir a trusted-key no arquivo named.conf
6. Incluir a trusted-key no arquivo /etc/trusted-key.key (teste dig)
7. Executar o BIND (named)
8. Realizar testes no servidor (DIG +sigchase)

Recomendação

Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos
http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/

Roteiro - Informações Importantes

registro.br
Registro de Domínios para a Internet no Brasil

Servidor Autoritativo

Reassinar a zona antes das assinaturas expirarem

Servidor Recursivo

Trocar a chave ancorada quando ocorrer um rollover do BR

nic.br

Parte III

Conclusão

registro.br
Registro de Domínios para a Internet no Brasil

Vulnerabilidades

- O Record NSEC é usado em DNSSEC para permitir a negação da existência
- De forma que para provar a inexistência, o NSEC aponta para o próximo nome existente na zona
- Esta prova de inexistência permite obter todo o conteúdo de uma zona com simples consultas de DNS

Varredura da Zona (Zone Walking)

- Até que este problema de varredura da zona esteja totalmente resolvido a zona **.com.br** não suportará DNSSEC

nic.br

registro.br
Registro de Domínios para a Internet no Brasil

Possíveis Soluções

- Uma solução proposta pela RFC 4470 é a assinatura online dos records sempre que necessário. Porém, não é viavel por exigir um processamento alto
- A IETF DNSEXT está trabalhando numa nova proposta denominada NSEC3 (draft-ietf-dnsext-nsec3)

registro.br
Registro de Domínios para a Internet no Brasil

NSEC3 - DNSSEC Hashed Authenticated Denial of Existence

- Soluciona o problema do "Zone Walking"
- Substitui o record NSEC pelo record NSEC3
- Faz um hash de todos os nomes da zona e ordena-os de forma canônica
- Ao invés de apontar para o próximo nome da zona, aponta para o próximo hash

Desvantagens com NSEC3

- Aumenta o processamento do servidor (diversas interações de hash)
- Para toda requisição é preciso calcular o hash a cada prova de não existência.

NSEC3 com OPT-out

Os records NSEC3 são gerados somente para records assinados, tornando as zonas menores

nic.br

registro.br
Registro de Domínios para a Internet no Brasil

Motivos para utilizar DNSSEC

- Impedir ataques do tipo "Man-in-The-Middle"
- Possibilitar um novo serviço de segurança pago aos seus clientes
- Assegurar-se de que seus dados estão chegando íntegros ao destino

Referências

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

Draft NSEC3 (draft-ietf-dnsext-nsec3)
DNSSEC Hashed Authenticated Denial of Existence

Referências

- DNSSEC.NET
  http://www.dnssec.net
- Wikipédia - DNSSEC
  http://pt.wikipedia.org/wiki/DNSSEC
- Wikipédia - Comparação entre softwares de servidores DNS
  http://en.wikipedia.org/wiki/Comparisonz_of_DNS_server_software
- Firewalls e DNS, como e porque configurar corretamente
  ftp://ftp.registro.br/pub/doc/dns-firewall.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/faq
- A última versão deste tutorial pode ser encontrada em
  ftp://ftp.registro.br/pub/doc/tutorial-DNSSEC.pdf

Agradecimento em especial

- DNSSEC – Olaf Kolkman (RIPE NCC/NLnet Labs)
  http://www.nlnetlabs.nl/dnssec_howto

Obrigado!