Tutorial DNSSEC [1]

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

Registro.br

4 de junho de 2009

[1] versão 1.5.1 (Revision: 5650)
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

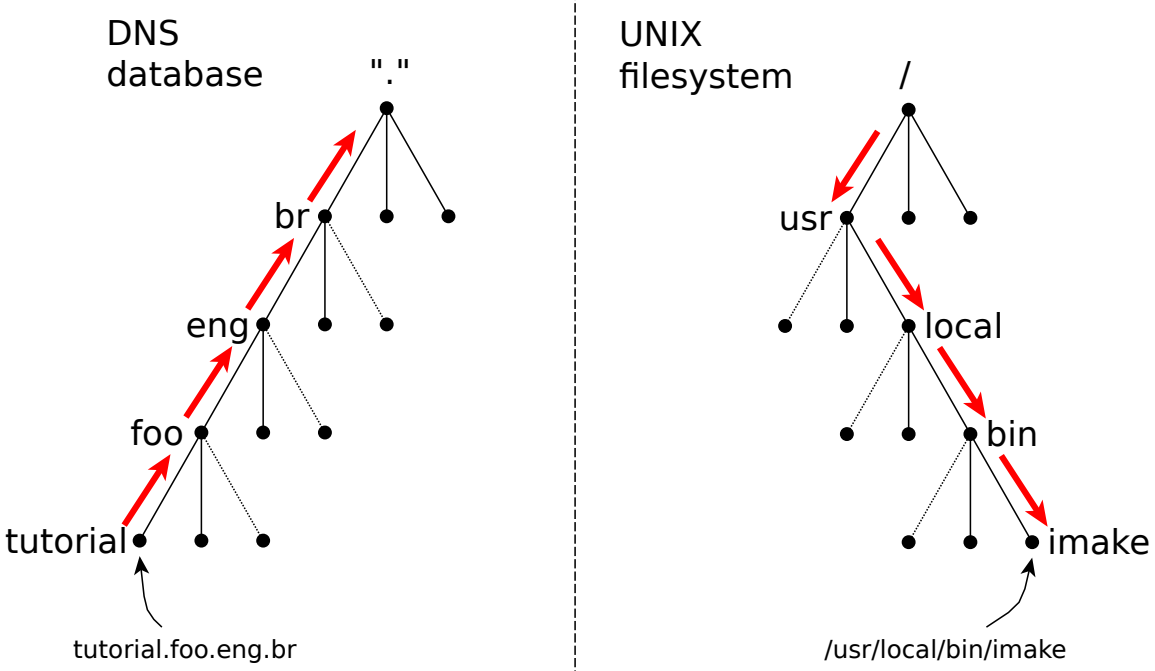
DNS - Domain Name System

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.

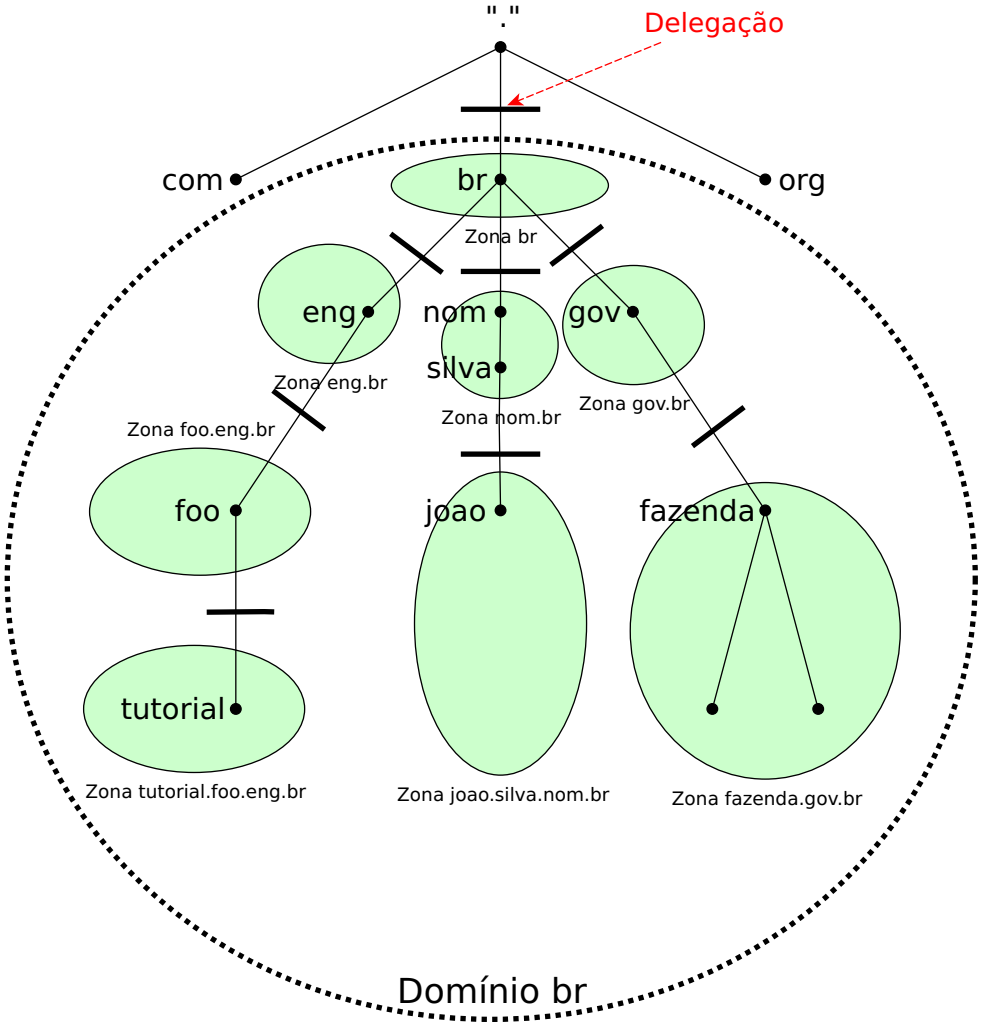
- Arquitetura hierárquica, dados dispostos em uma árvore invertida
- Distribuída eficientemente, sistema descentralizado e com cache
- O principal propósito é a resolução de nomes de domínio em endereços IP e vice-versa

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

Hierarquia


DNS
database
"."
br
eng
foo
tutorial
tutorial.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.

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 (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

Exemplo de records de uma zona

registro.br
Registro de Domínios para a Internet no Brasil

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

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

Apêndice I - SOA

Tipos de servidores

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, responde um endereço caso possua, uma referência caso conheça o caminho da resolução ou uma negação caso não conheça

Exemplo de requisição de endereço

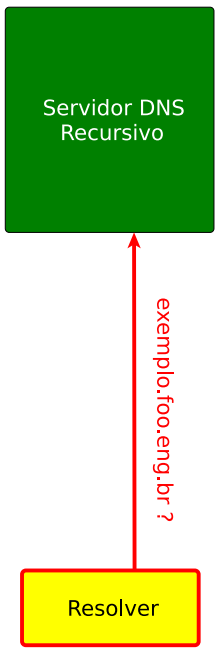
Supondo que o cache esta vazio ou sem informações de br, eng.br, foo.eng.br, exemplo.foo.eng.br

Resolver

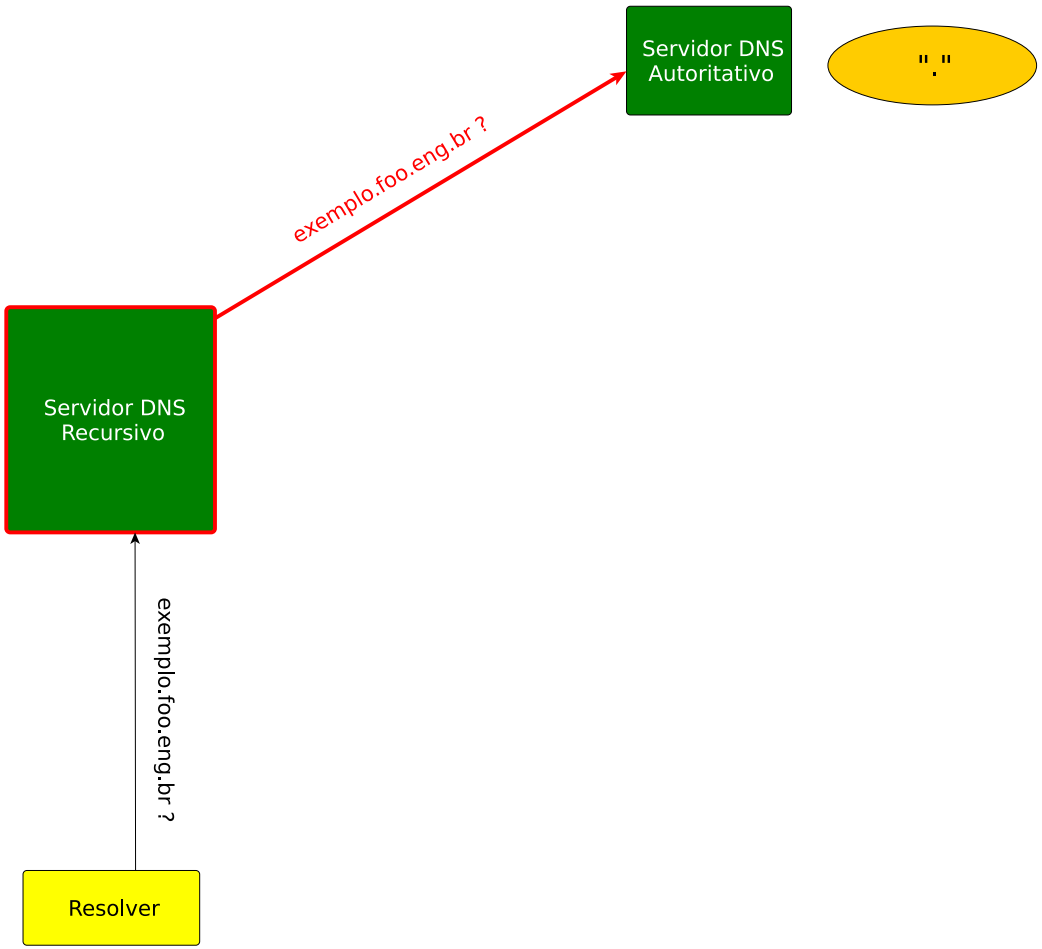
Serviço localizado no cliente que tem como responsabilidade resolver as requisições DNS para diversos aplicativos

Exemplo de requisição de endereço

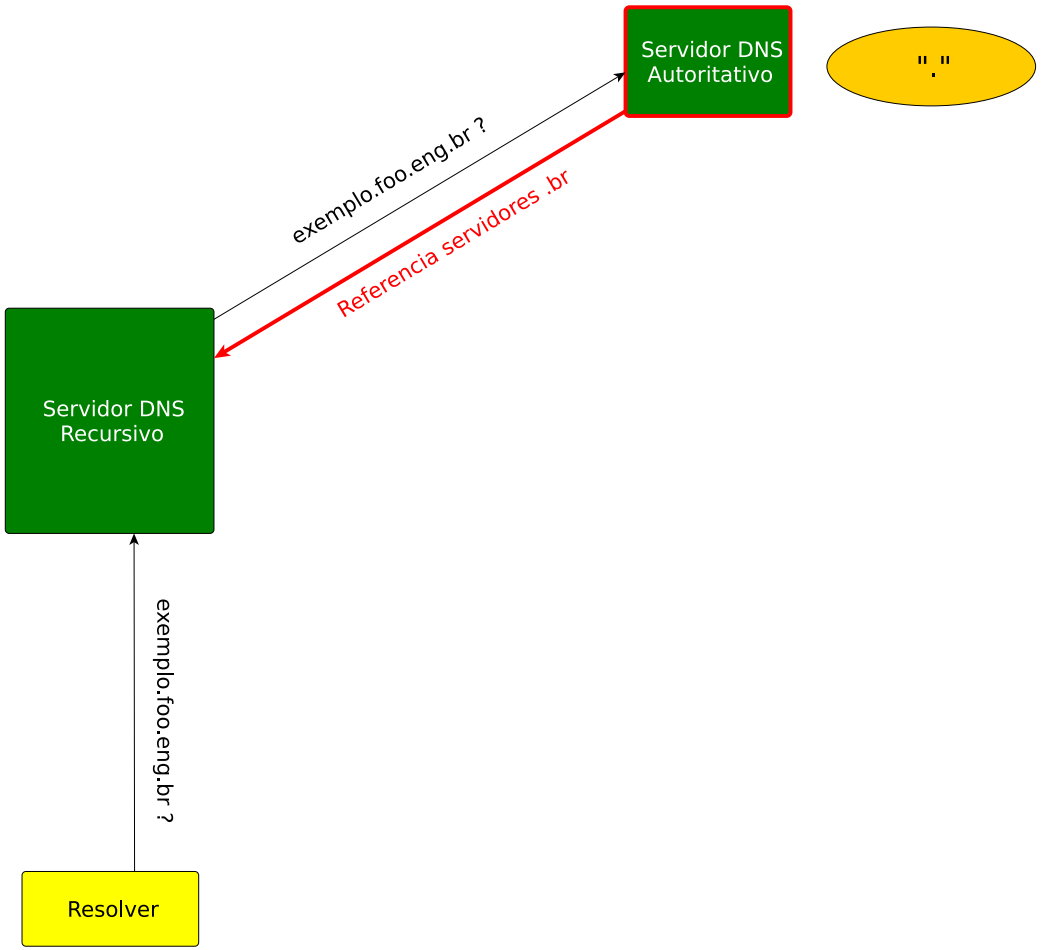
Supondo que o cache está vazio ou sem informações de br, eng.br, foo.eng.br, exemplo.foo.eng.br



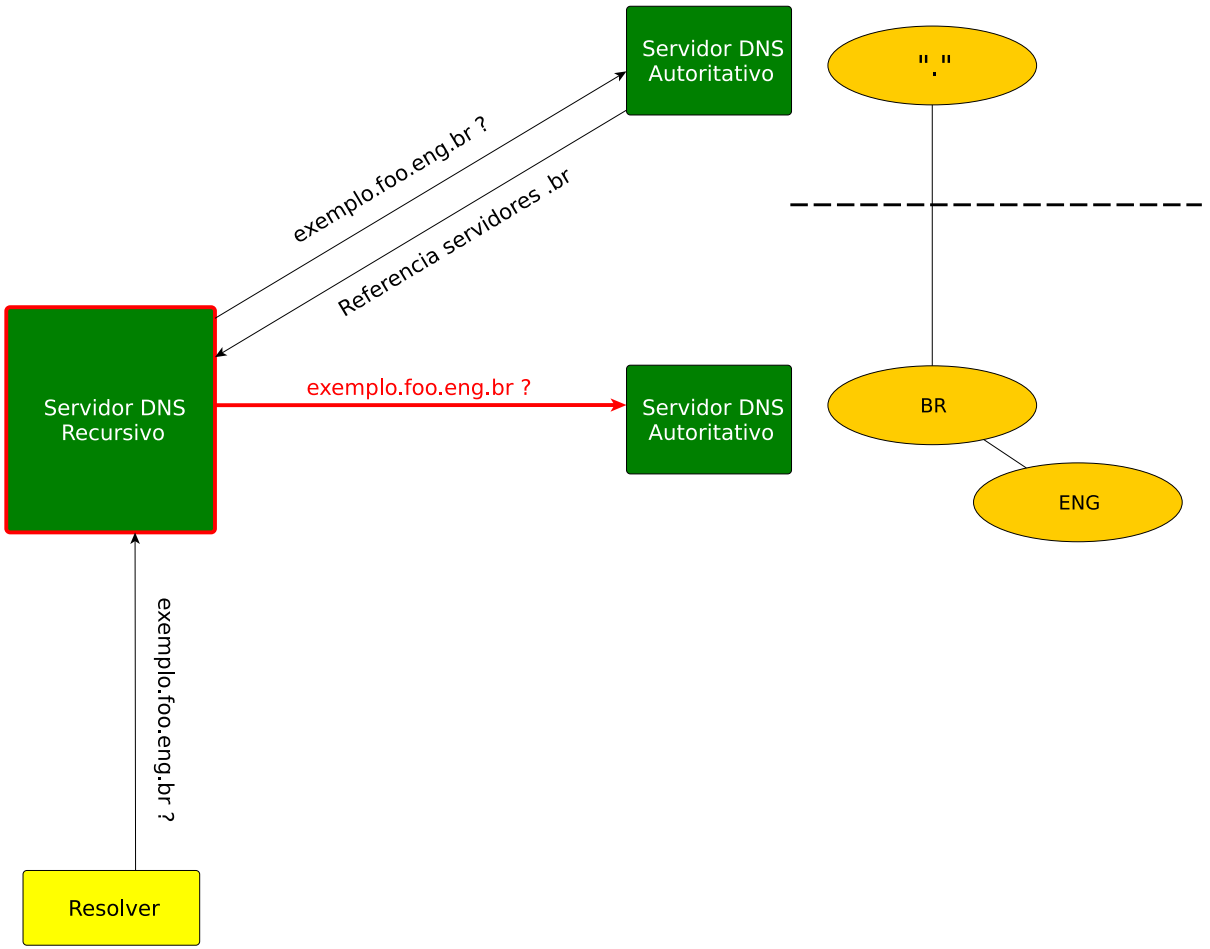
Exemplo de requisição de endereço



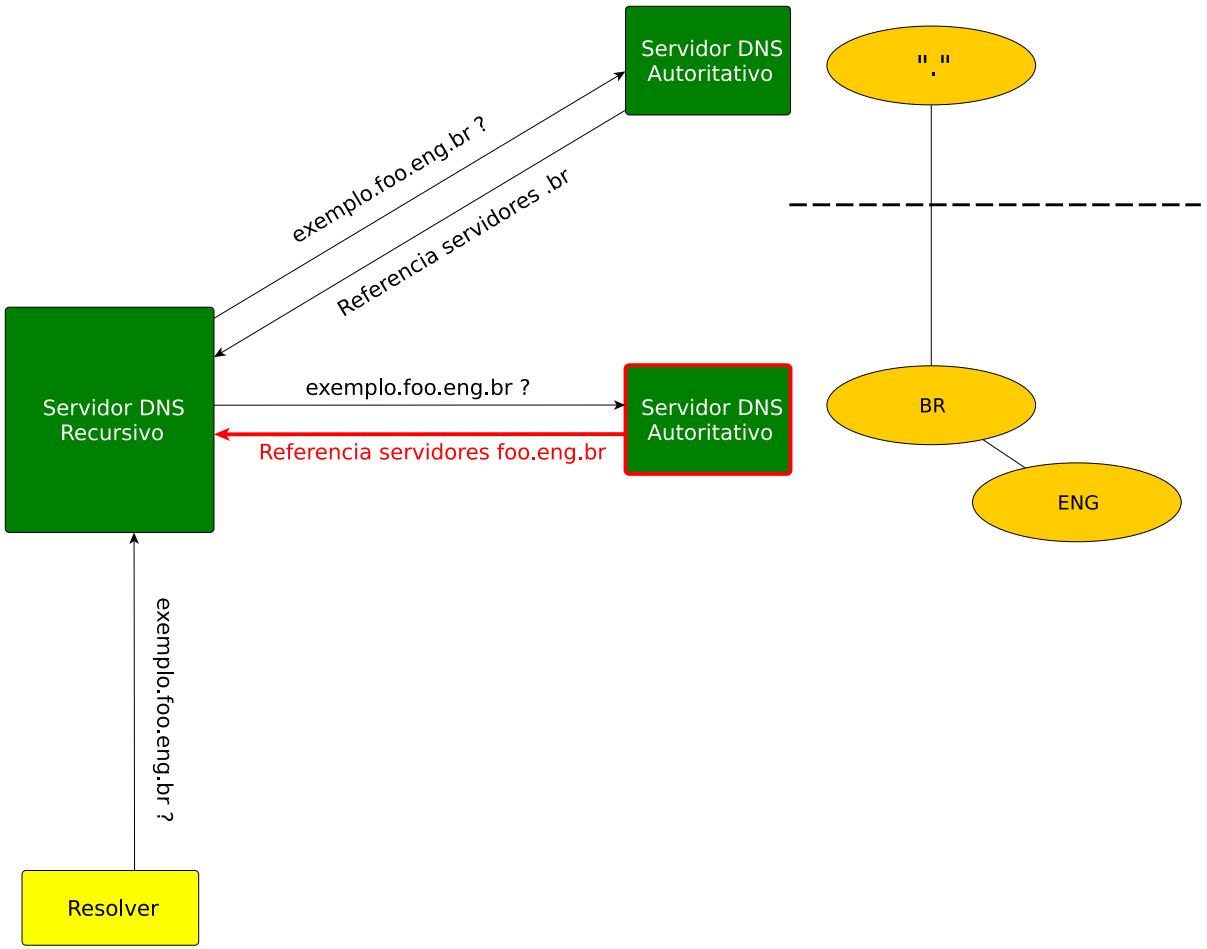
Exemplo de requisição de endereço



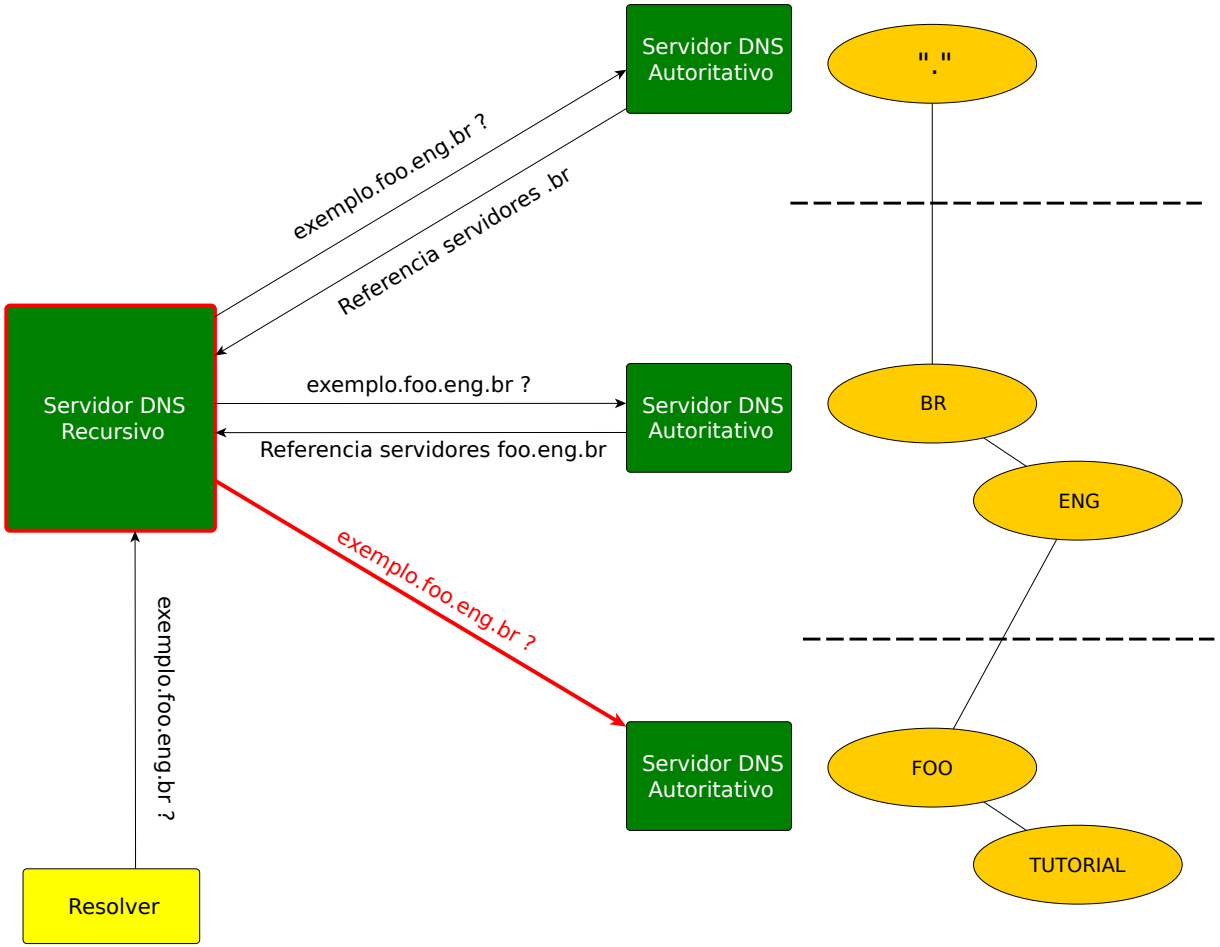
Exemplo de requisição de endereço



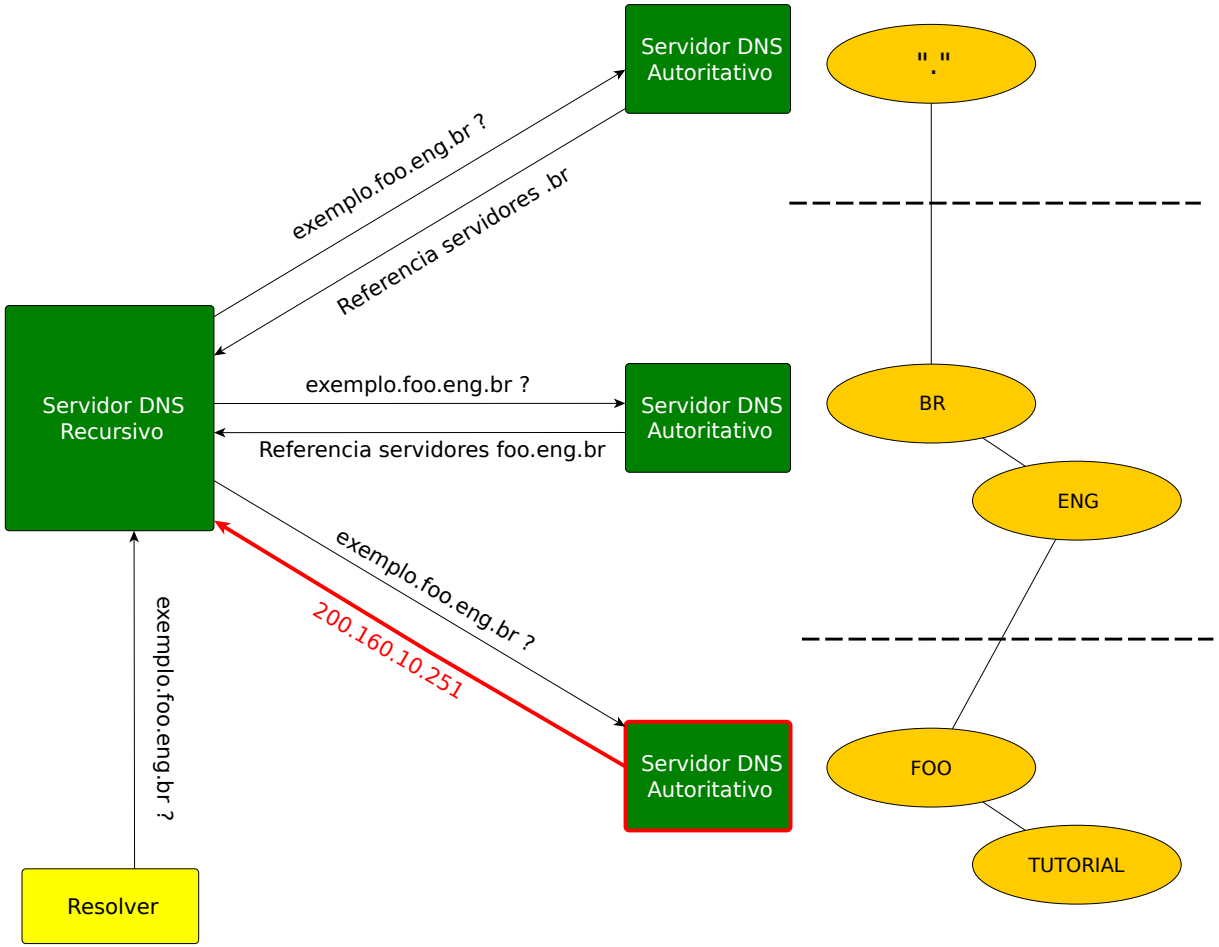
Exemplo de requisição de endereço



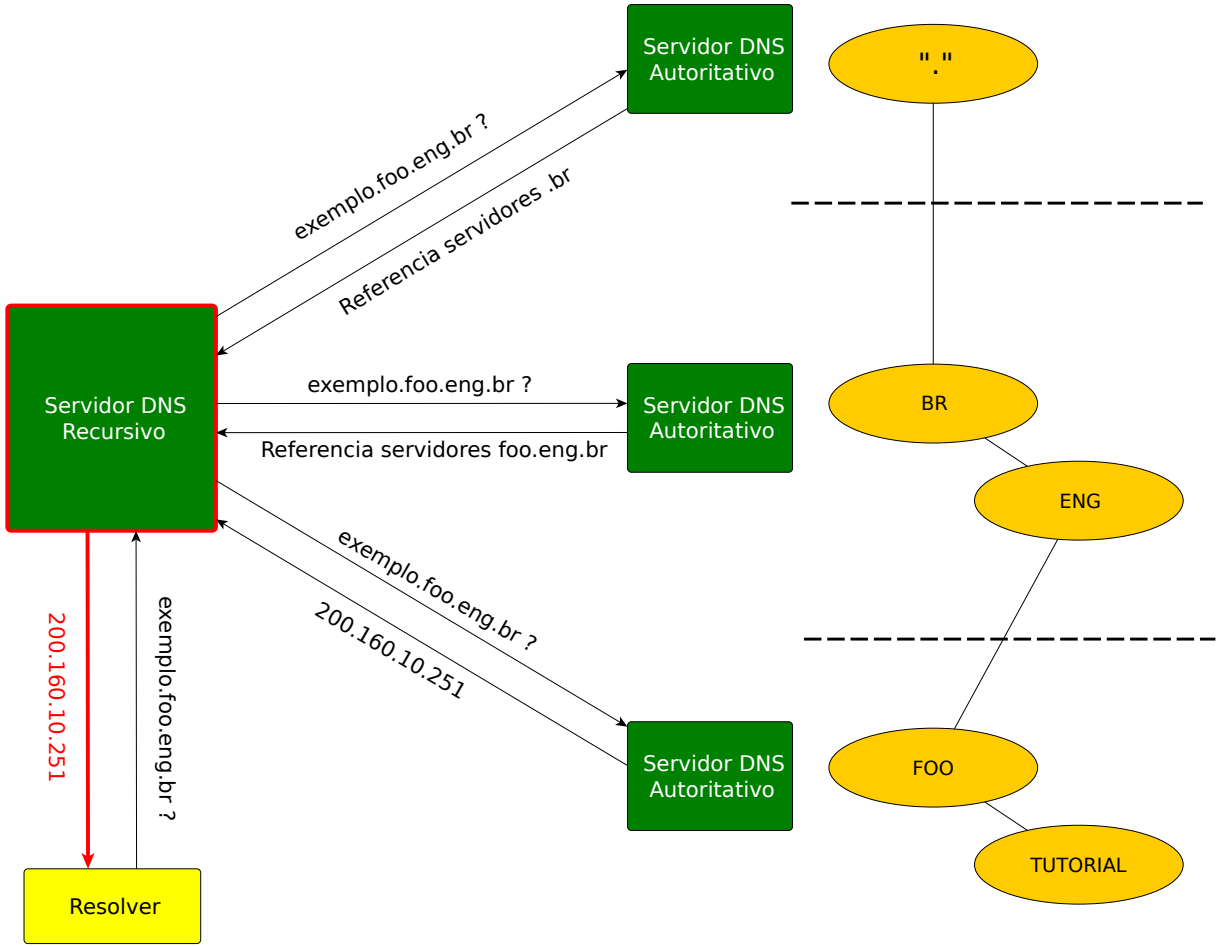
Exemplo de requisição de endereço



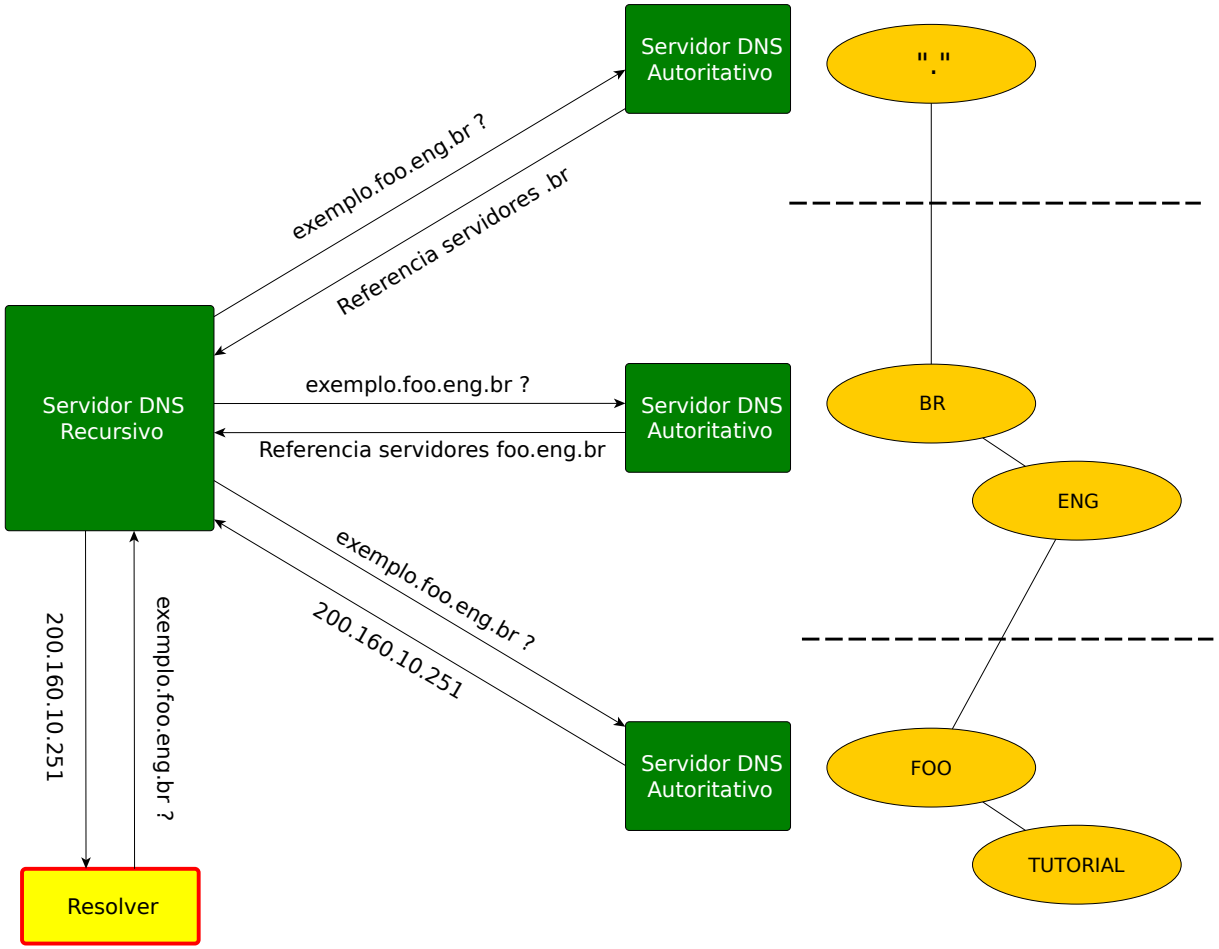
Exemplo de requisição de endereço



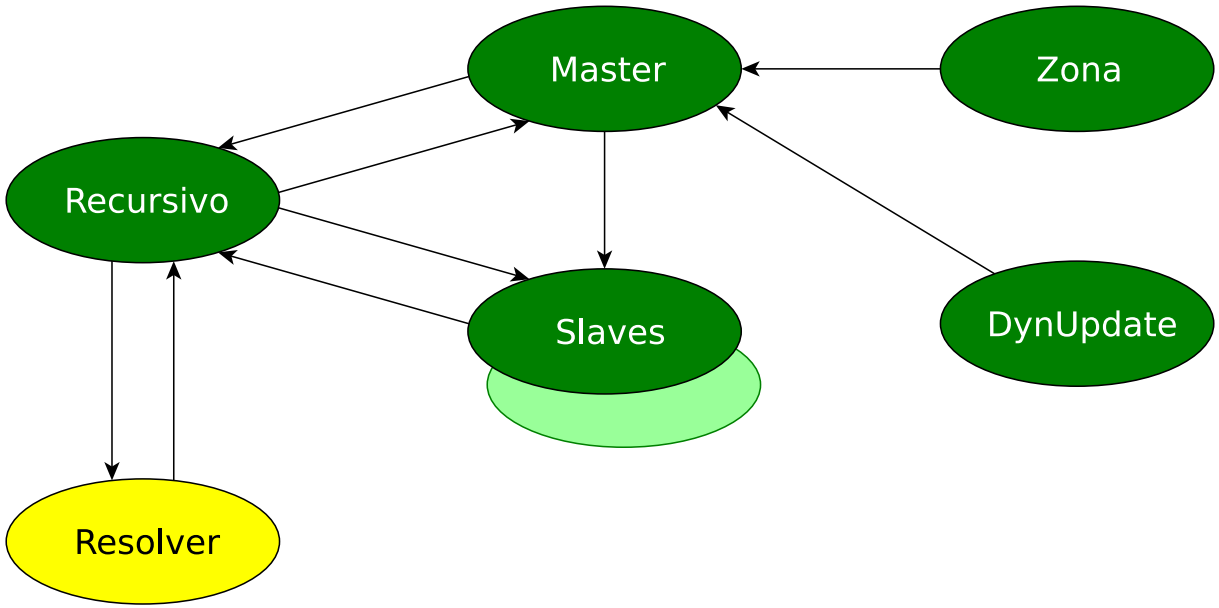
Exemplo de requisição de endereço



Exemplo de requisição de endereço

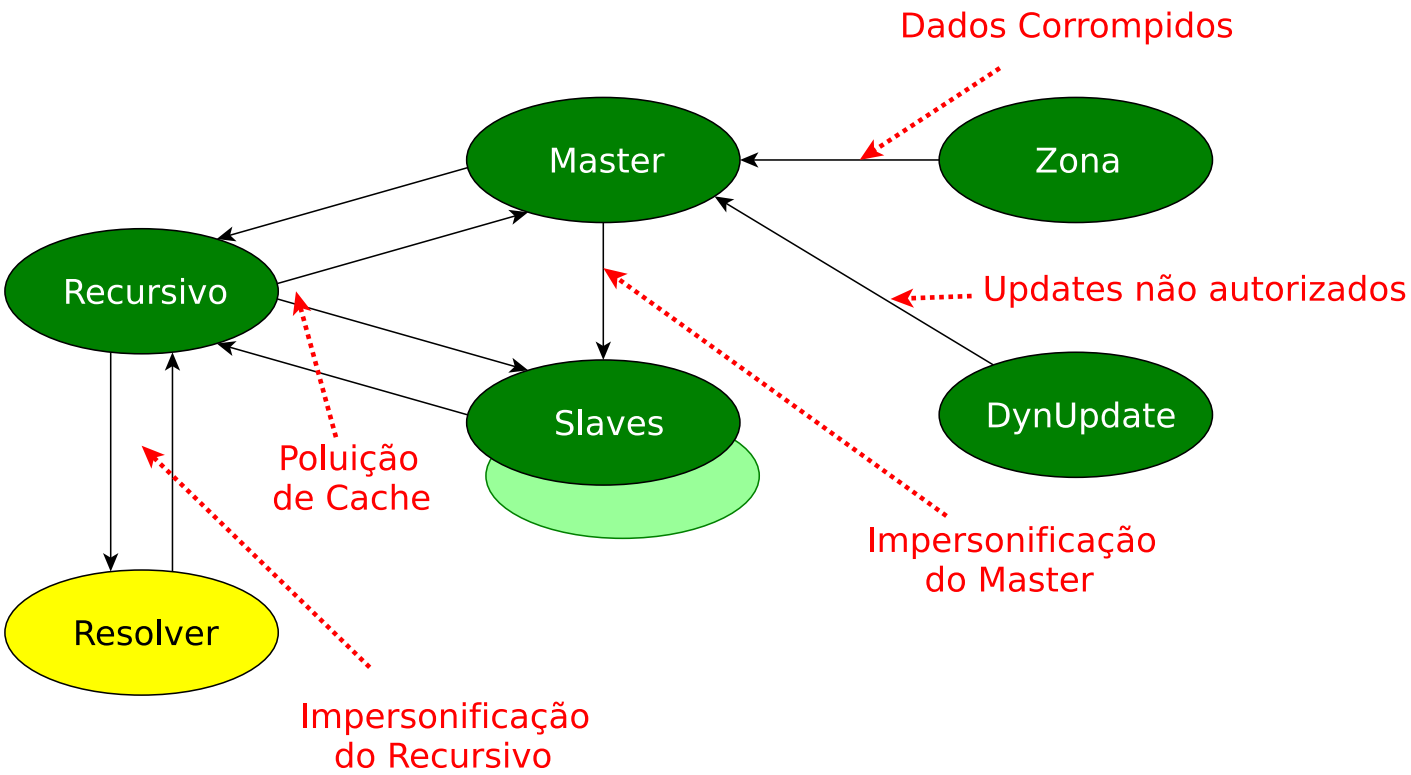


Fluxo de dados

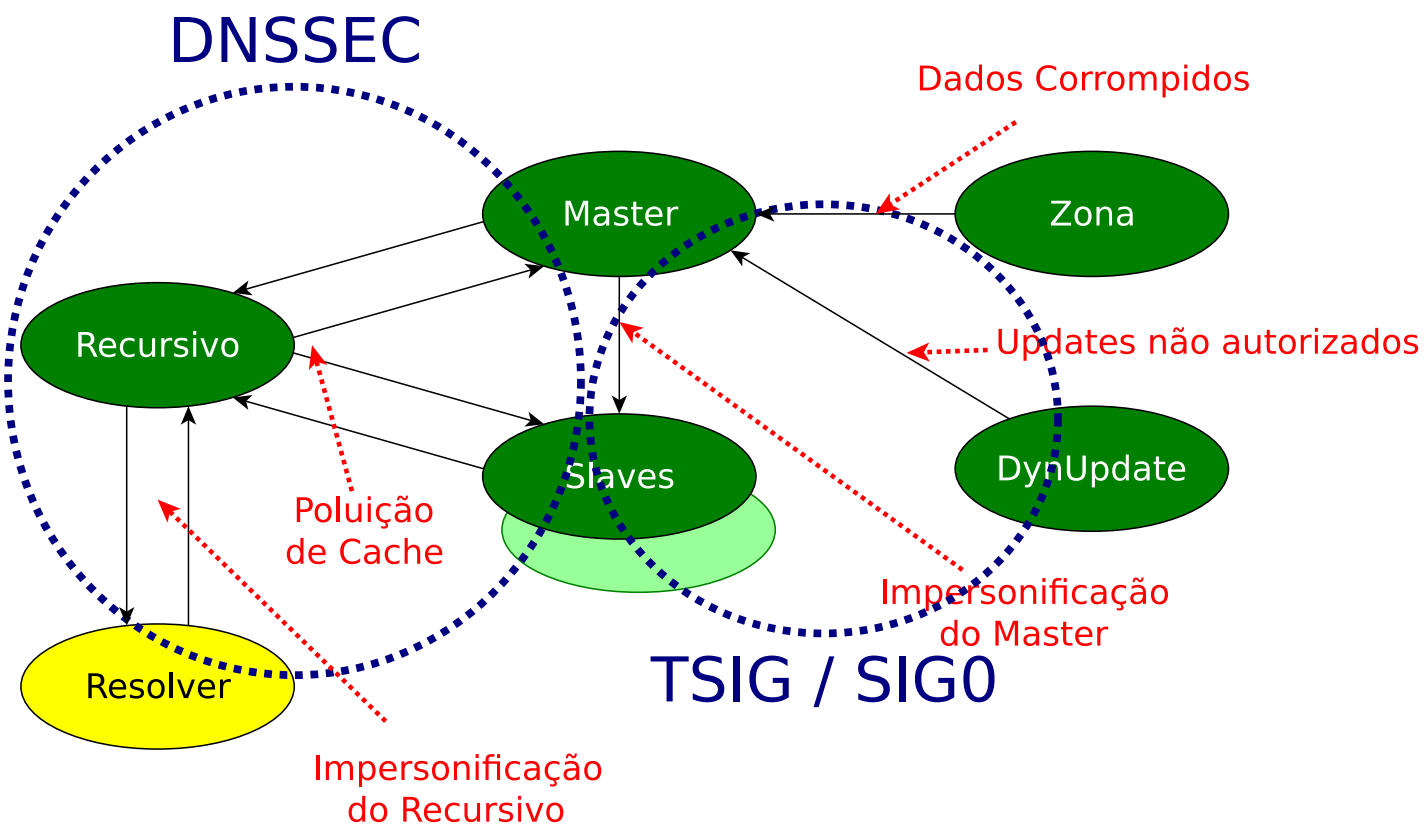


1. Resolver faz consultas no Recursivo
2. Recursivo faz consultas no Master ou Slave
3. Master tem a zona original (via arquivo ou Dynamic Update)
4. Slave recebe a zona do Master (AXFR ou IXFR)

Vulnerabilidades



Soluções


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

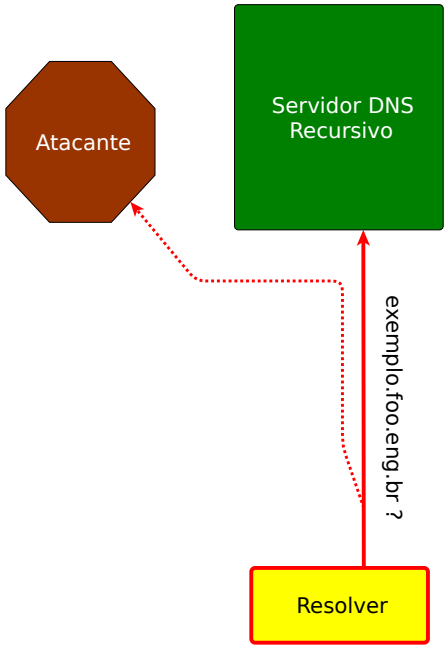
Exemplo de Ataque 1

Man-in-The-Middle

Resolver

Exemplo de Ataque 1

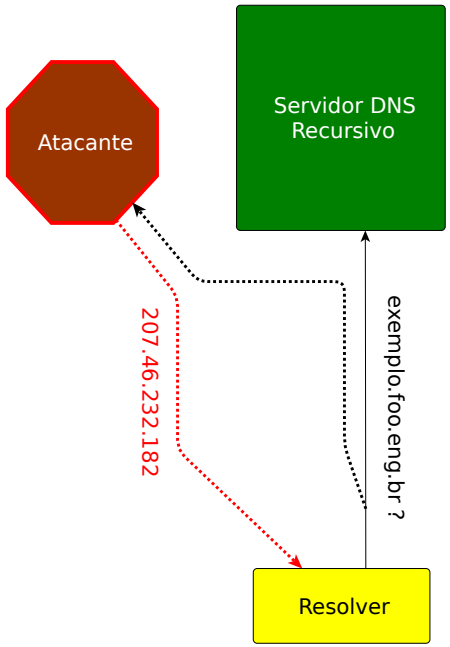
Man-in-The-Middle



Exemplo de Ataque 1

Man-in-The-Middle

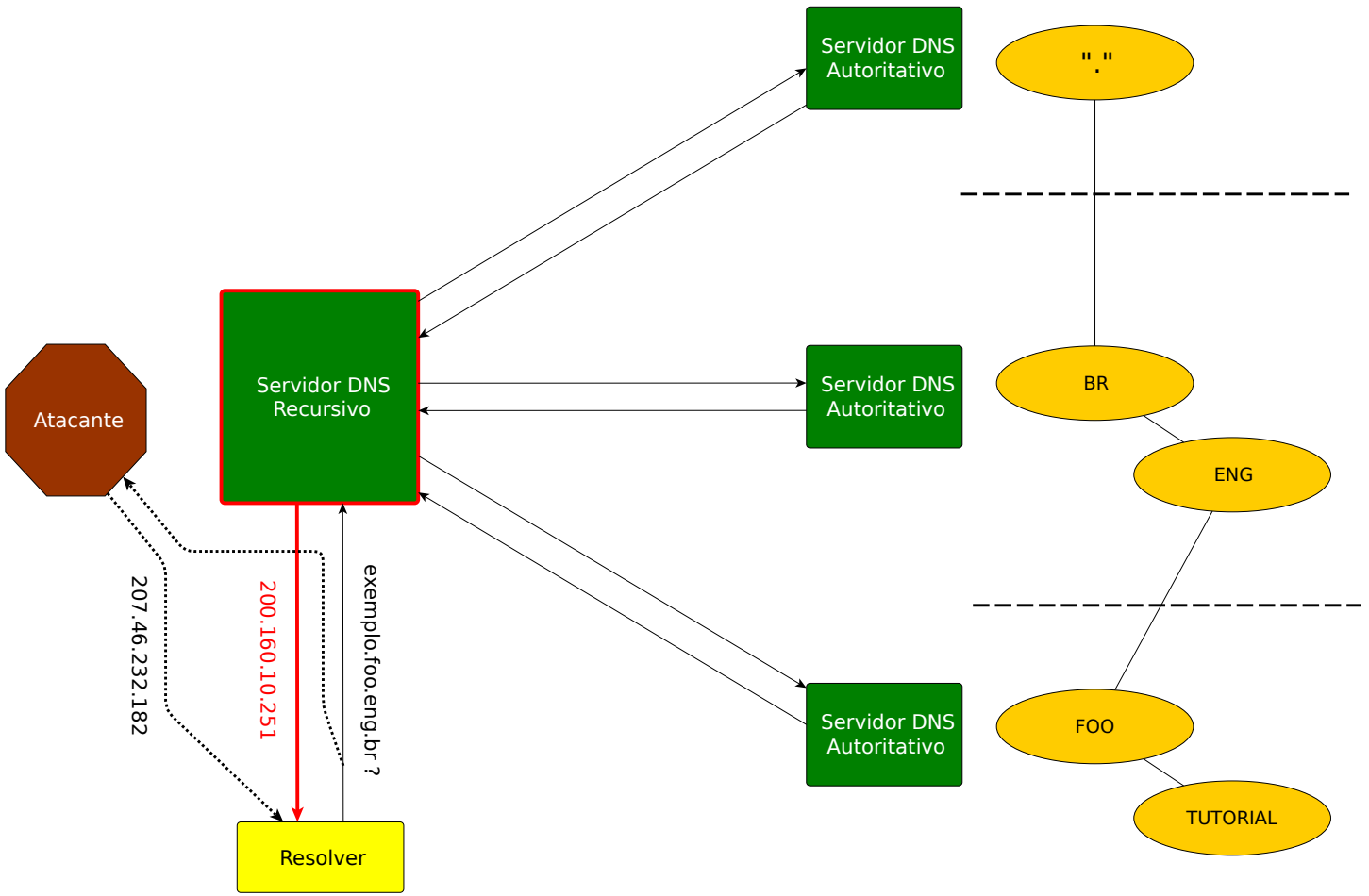
O atacante responde mais rápido, spoofando endereço do recursivo



Exemplo de Ataque 1

Man-in-The-Middle

O atacante responde mais rápido, spoofando endereço do recursivo

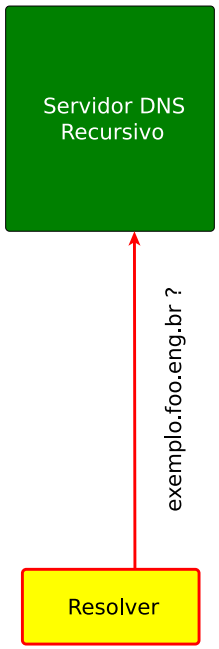


Exemplo de Ataque 2

Poluição de Cache

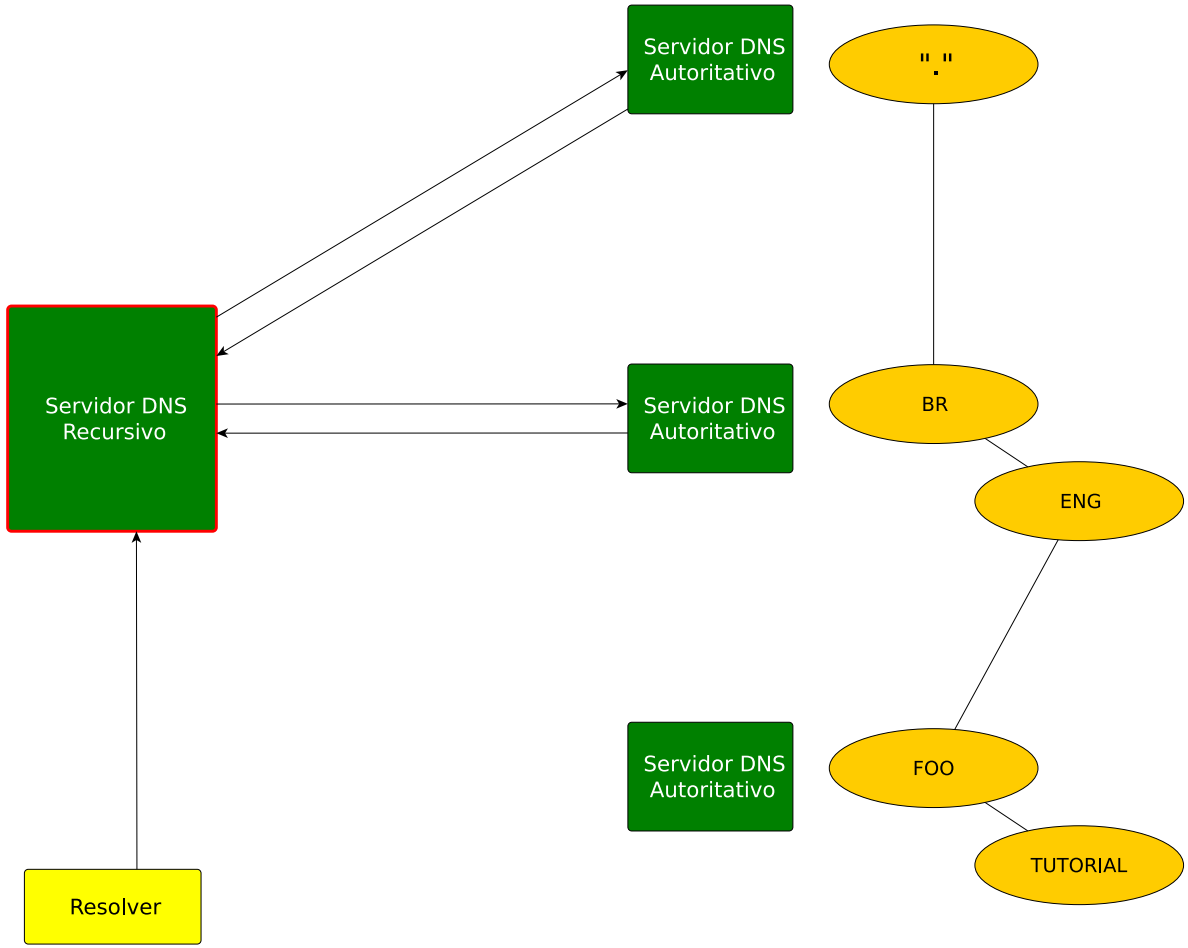
Resolver

Exemplo de Ataque 2
Poluição de Cache



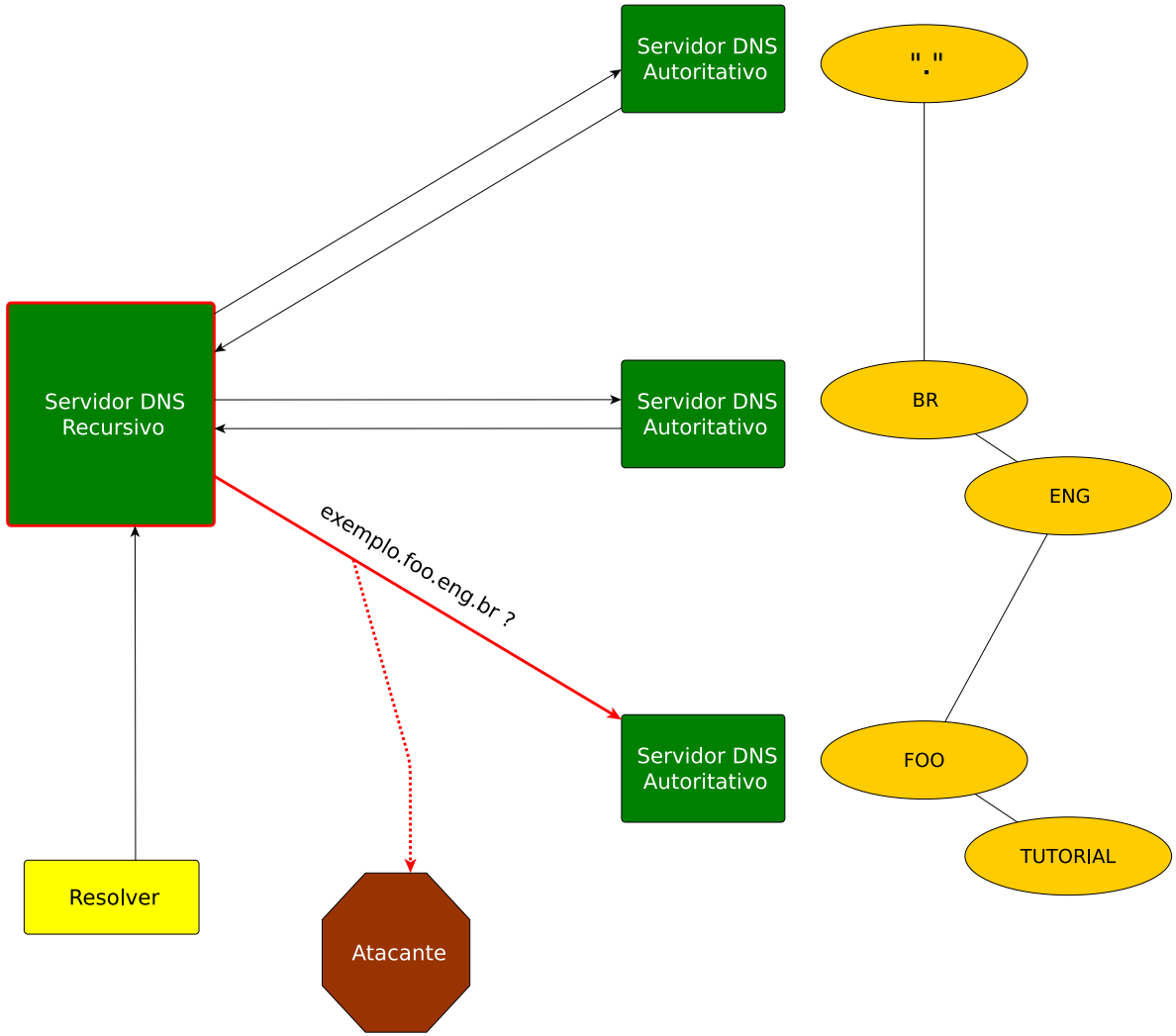
Exemplo de Ataque 2

Poluição de Cache



Exemplo de Ataque 2

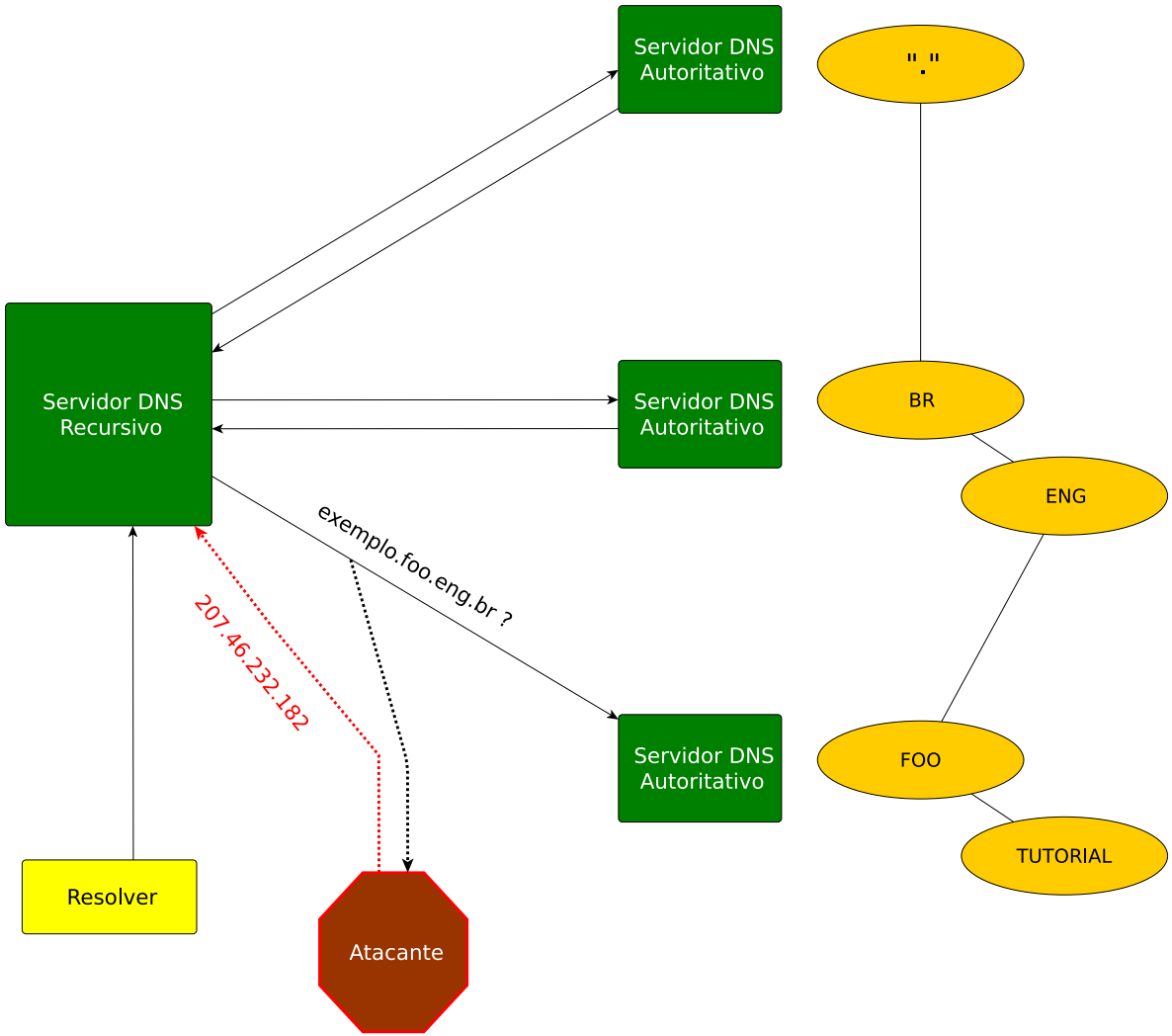
Poluição de Cache



Exemplo de Ataque 2

Poluição de Cache

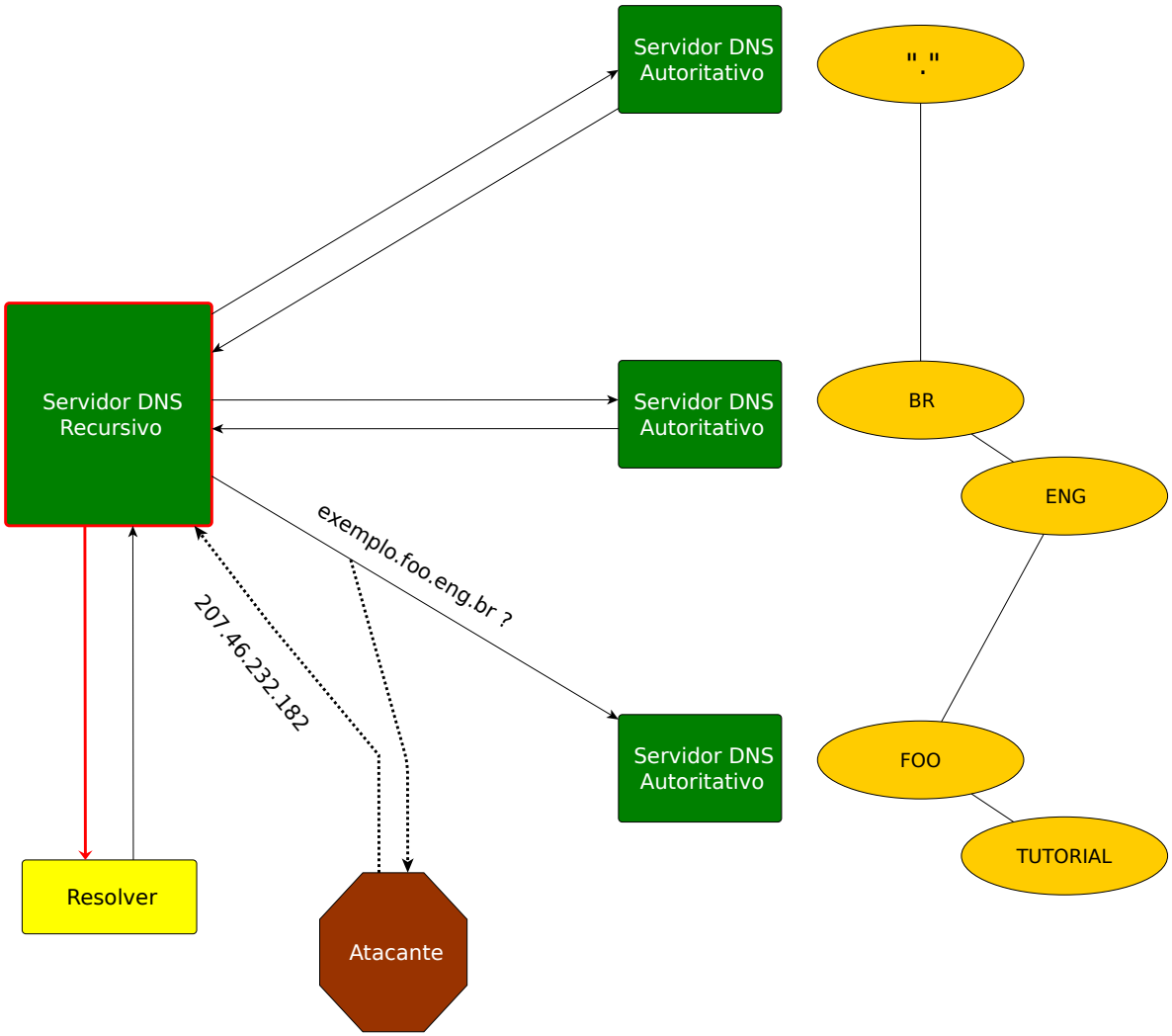
O atacante responde mais rápido, spoofando endereço do autoritativo



Exemplo de Ataque 2

Poluição de Cache

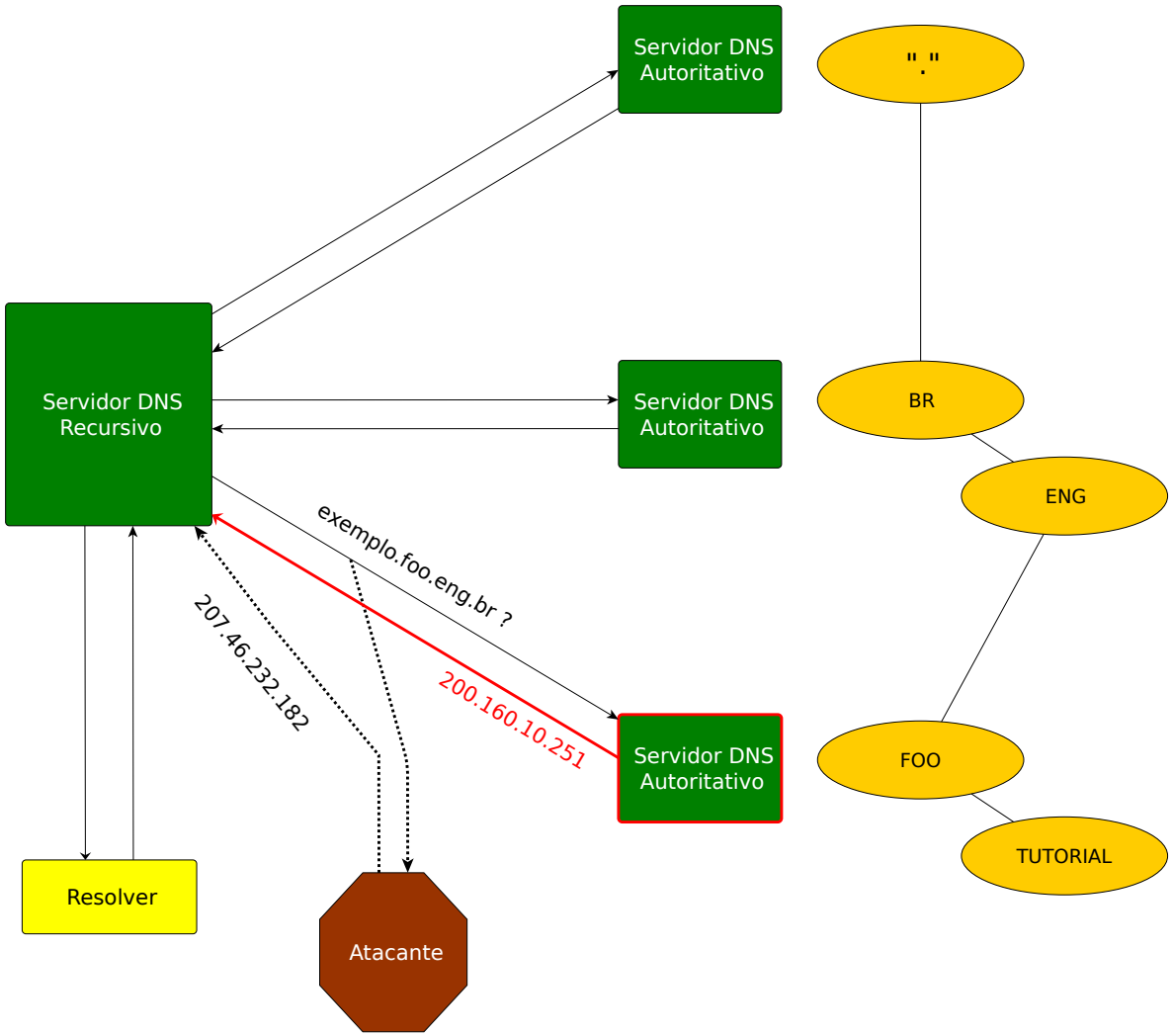
O atacante responde mais rápido, spoofando endereço do autoritativo



Exemplo de Ataque 2

Poluição de Cache

O atacante responde mais rápido, spoofando endereço do autoritativo



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 na versão denominada DNSSEC bis com opcional NSEC3

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

Avanço de DNSSEC no Mundo

registro.br
Registro de Domínios para a Internet no Brasil

World Wide DNSSEC Deployment

See also DNSSEC Theory and World Wide Deployment by Paul Wouters, November 21, 2007, SecTor

This map was created by Paul Wouters

fonte: http://www.xelerance.com/dnssec/

nic.br

registro.br
Registro de Domínios para a Internet no Brasil

Quem pode utilizar DNSSEC abaixo do .br?

Todos os domínios abaixo do .br podem (e devem) utilizar DNSSEC.

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

Utilização de DNSSEC

registro.br
Registro de Domínios para a Internet no Brasil

Quem pode utilizar DNSSEC abaixo do .br?

Todos os domínios abaixo do .br podem (e devem) utilizar DNSSEC.

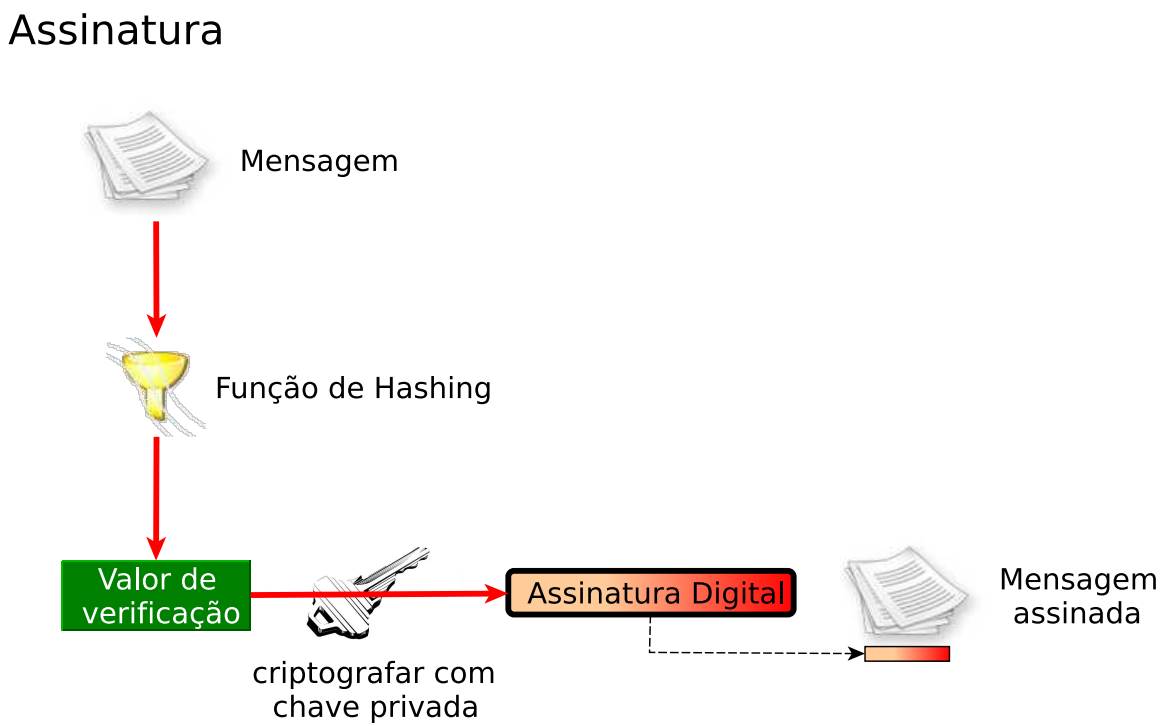
Mais informações podem ser obtidas no site http://www.registro.br/info/dpn.html

Onde DNSSEC é Obrigatório?

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

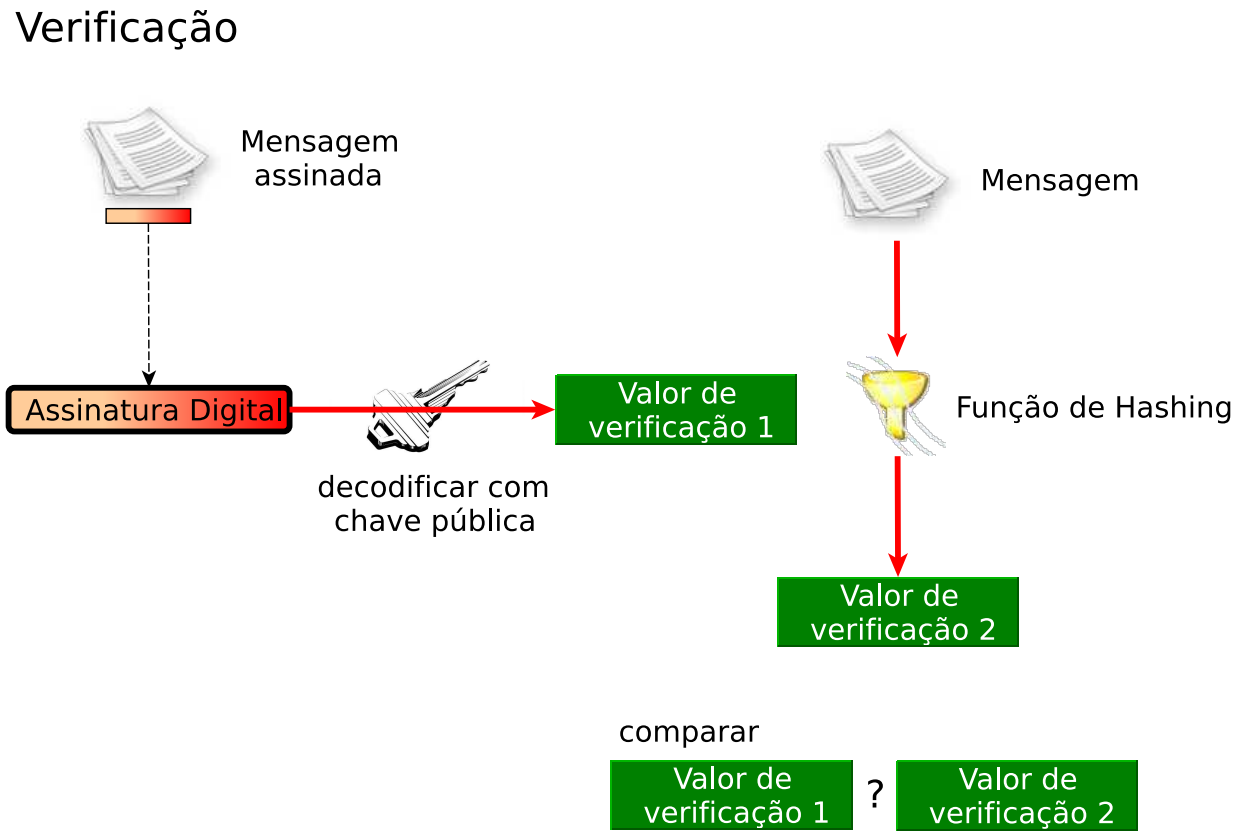
nic.br

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

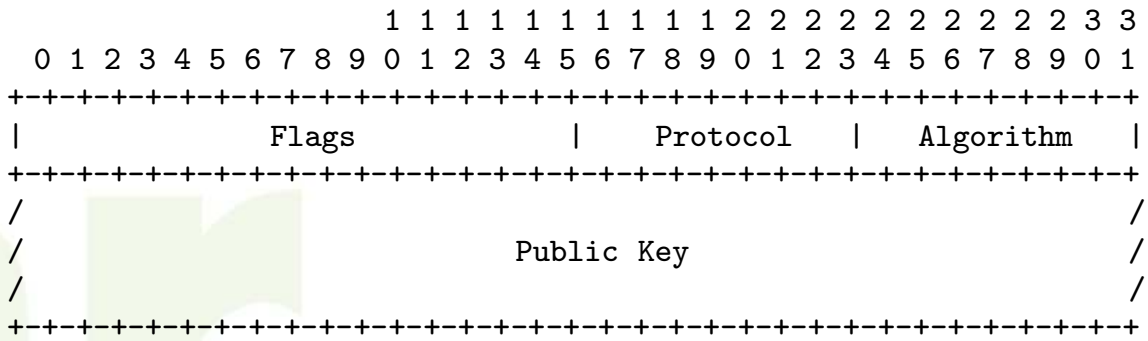
registro.br
Registro de Domínios para a Internet no Brasil

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

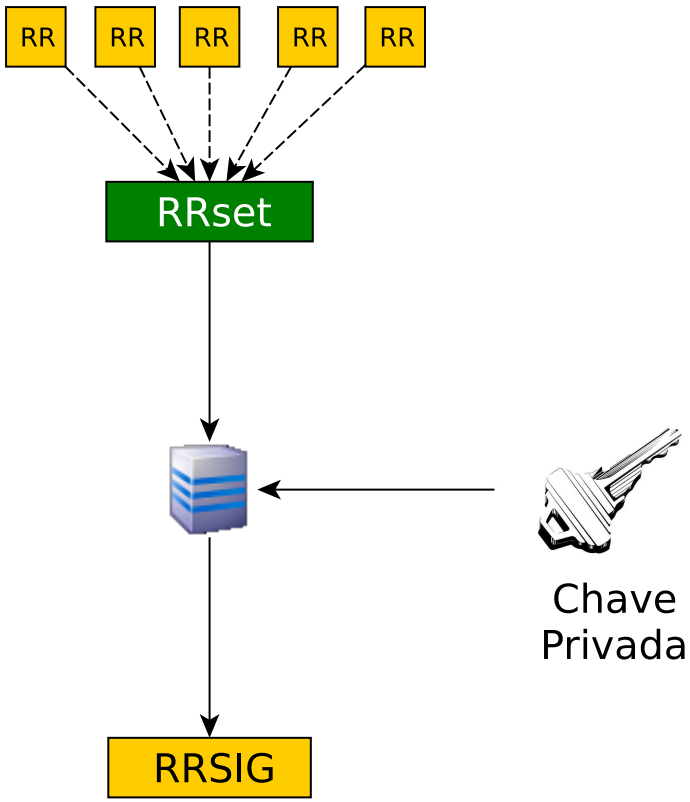


Exemplo

```
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)



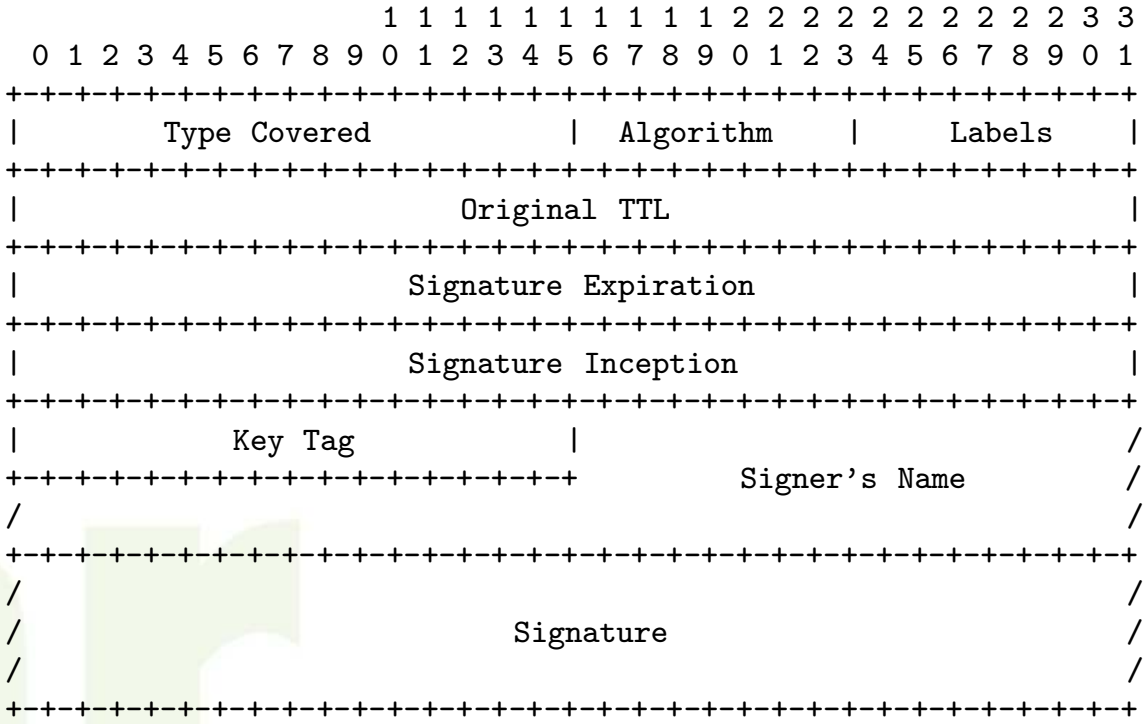
Exemplos de RRset:

```
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

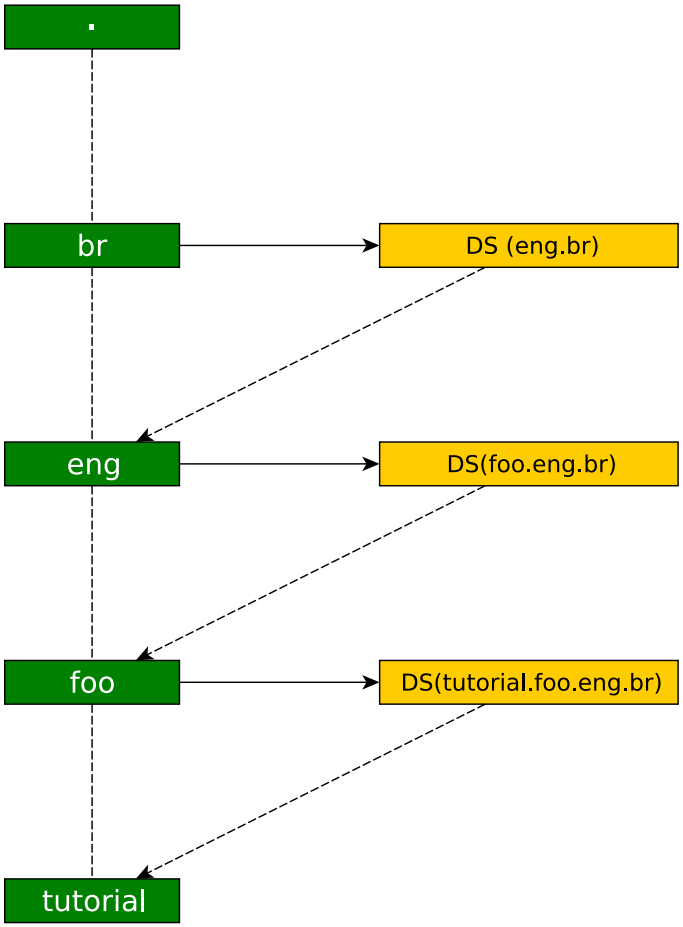
Serve para informar que existem uma cadeia de confiança entre um domínio e seus sub-domínios.

Indica:

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

A zona Pai tem autoridade pelo registro DS

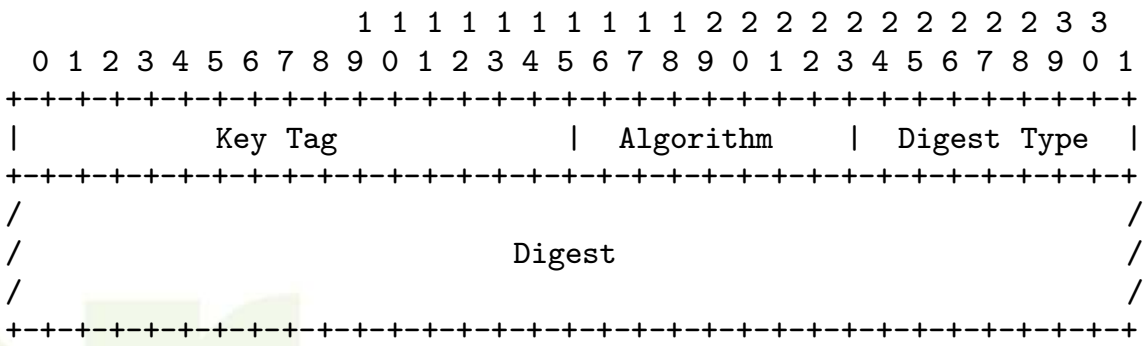
- Os registros NS são apenas "hints" e não são autoritativos no Pai
- O record DS **não** deve aparecer no Filho



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 (DNSSEC Lookaside Validation – slide **??**)

DS



Exemplo

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

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

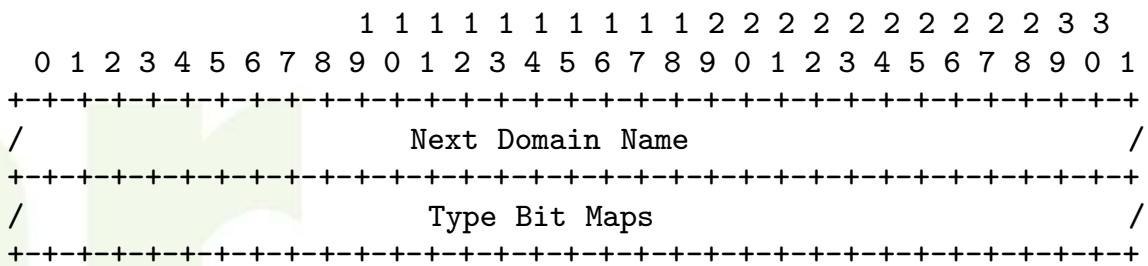
Exemplo de DS pelo Whois

```
$ 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=
```

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

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 à zona

Ancorar Chave - Servidor Recursivo

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

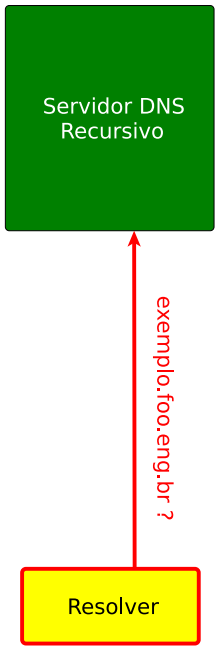
Isto serve para associar o inicio da cadeia de confiança a um ponto seguro.

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

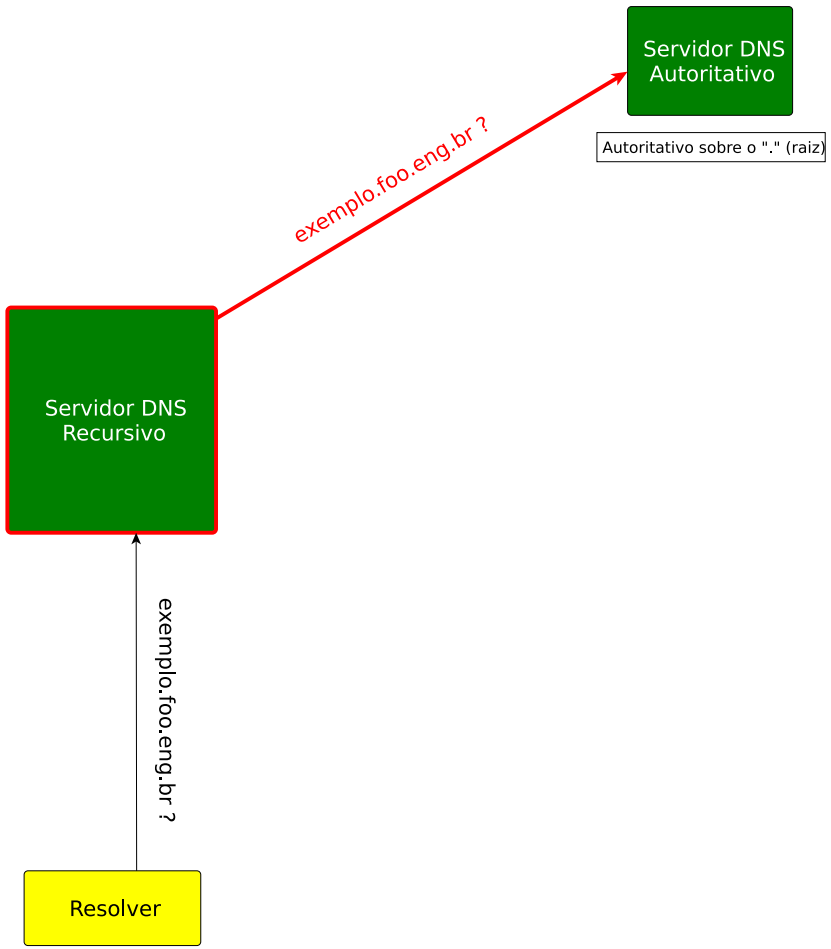
- **.BR** `https://registro.br/ksk/`

Exemplo

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

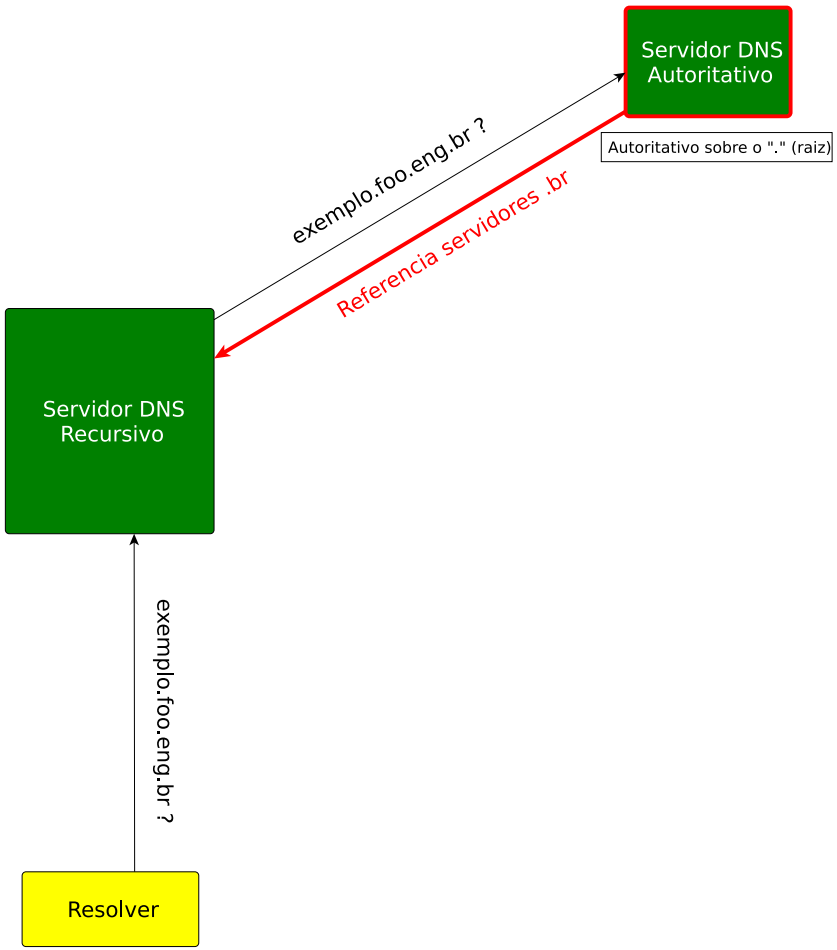


Exemplo



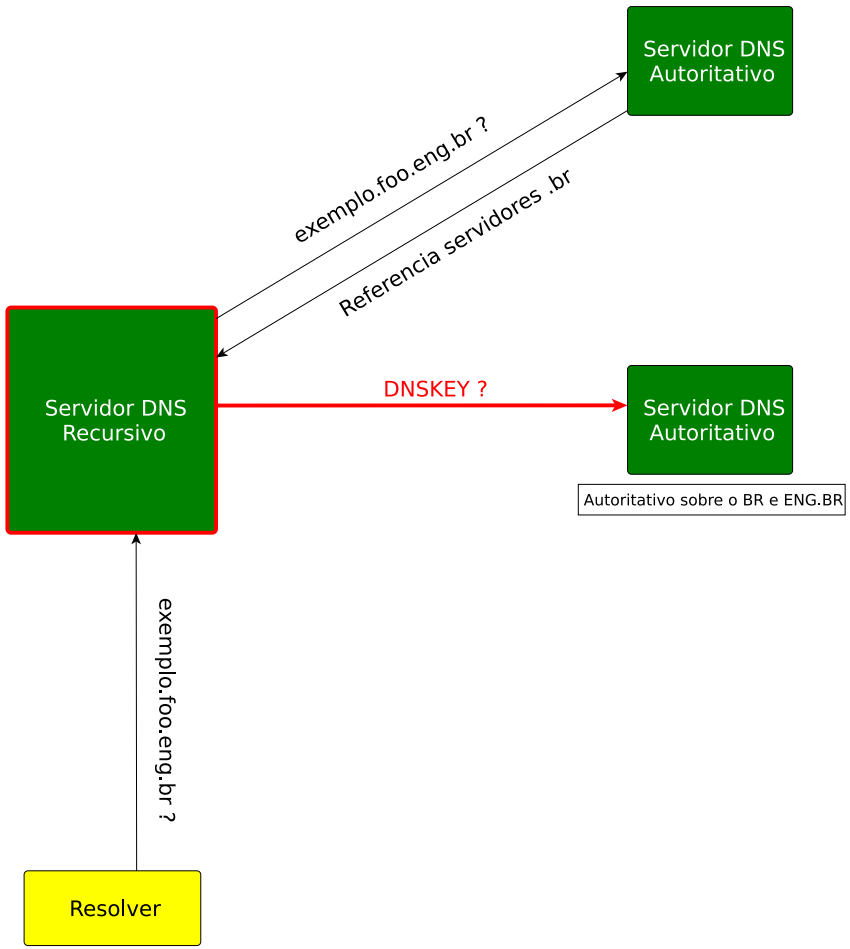
- Nesta simulação de resolução supomos que a raiz não está assinada.

Exemplo



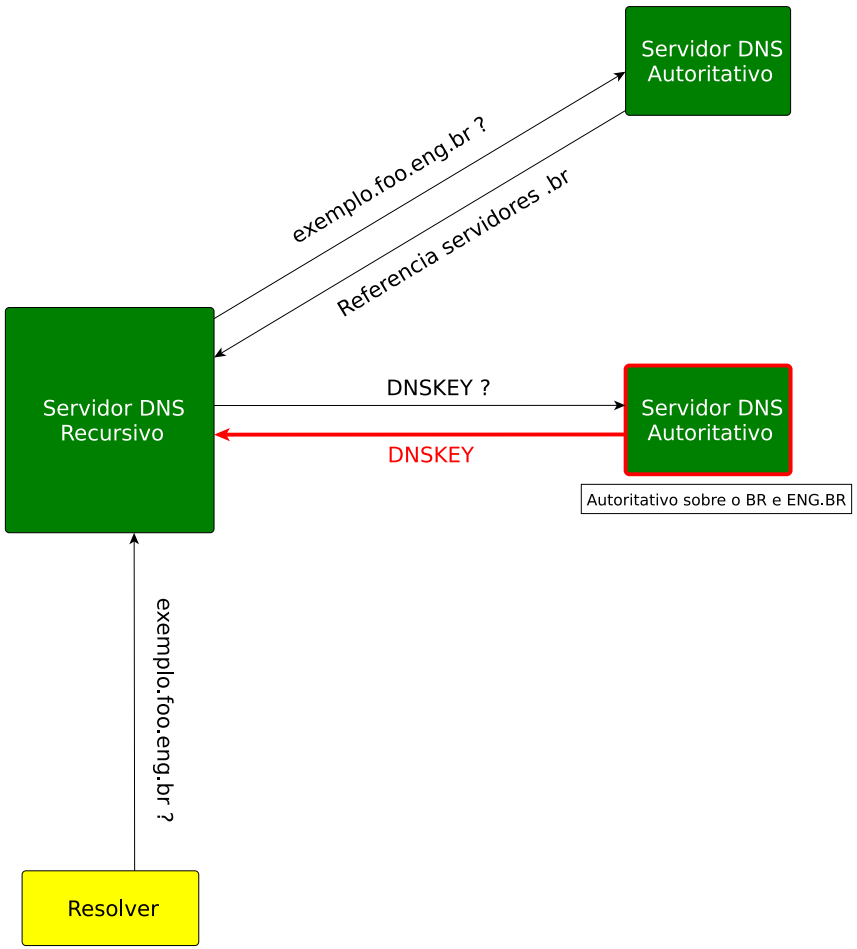
- Retorna sem resposta, mas com referência para os Records: NS do “.br”.

Exemplo



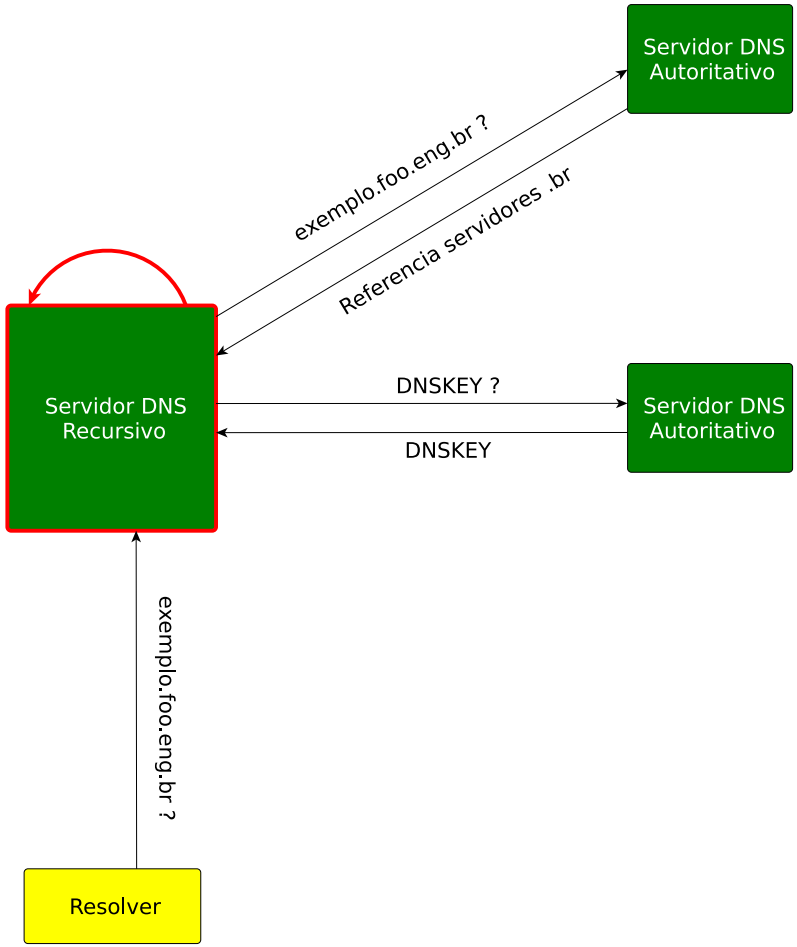
- O servidor recursivo requisita a DNSKEY ao verificar que o nome da zona é igual ao nome da zona que consta em sua trusted-key.

Exemplo



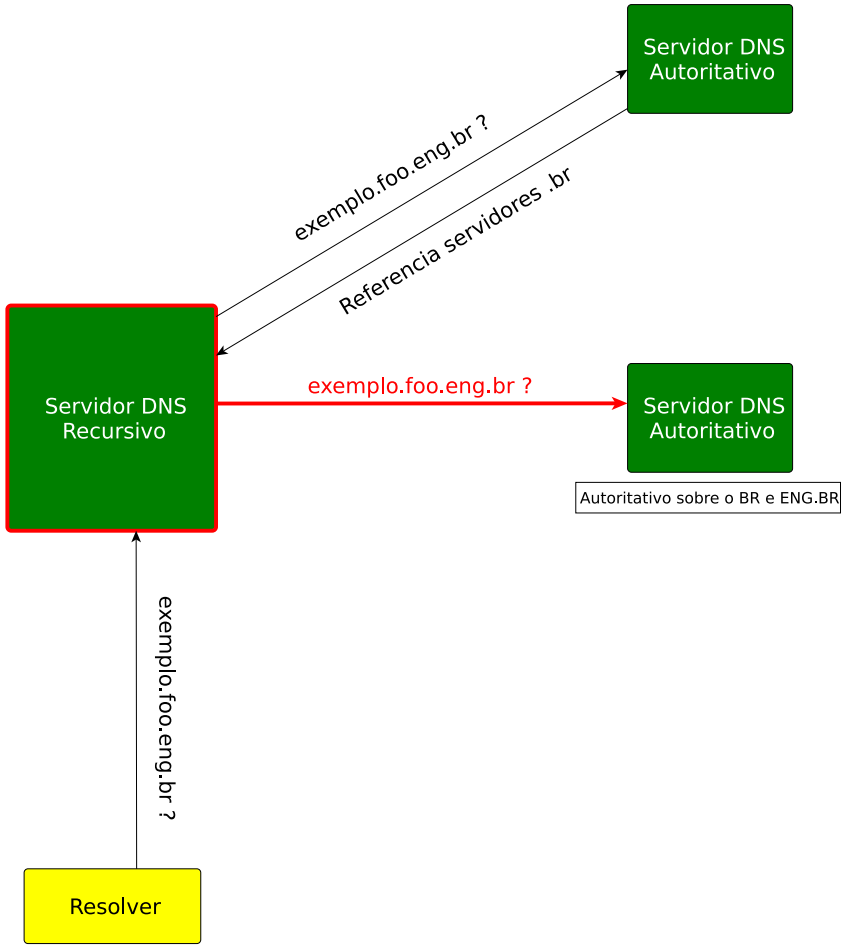
- O servidor DNS responde enviando DNSKEY e o RRSIG

Exemplo

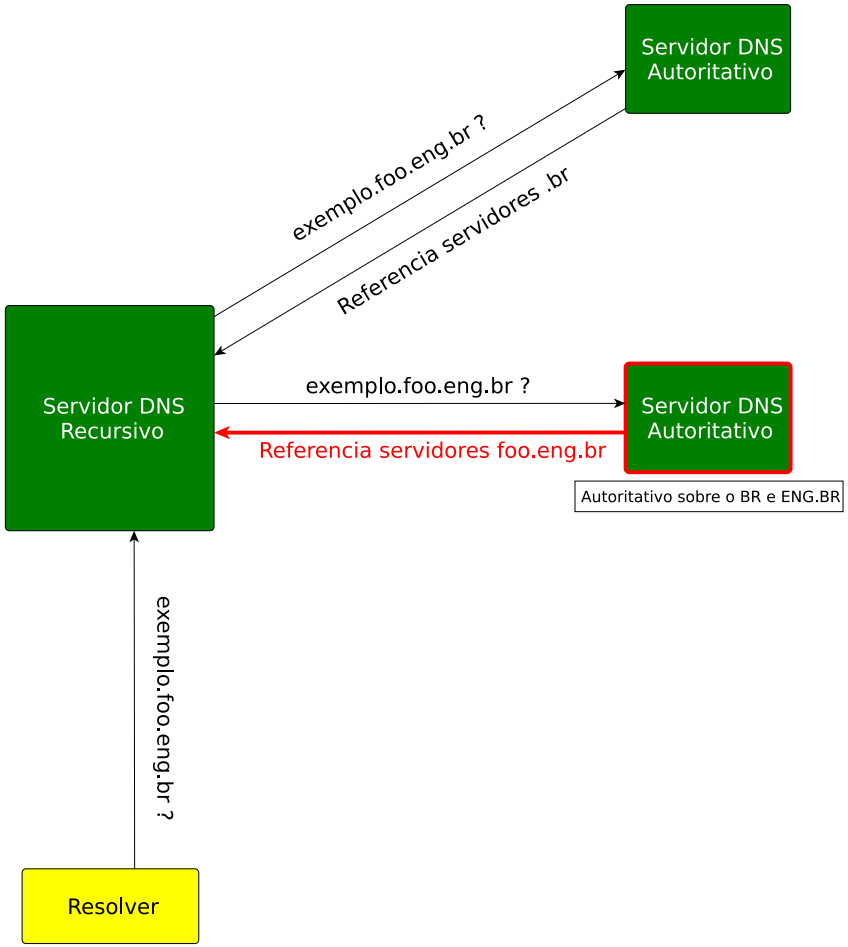


- Compara a trusted-key com a DNSKEY, caso for válida continua com as requisições

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

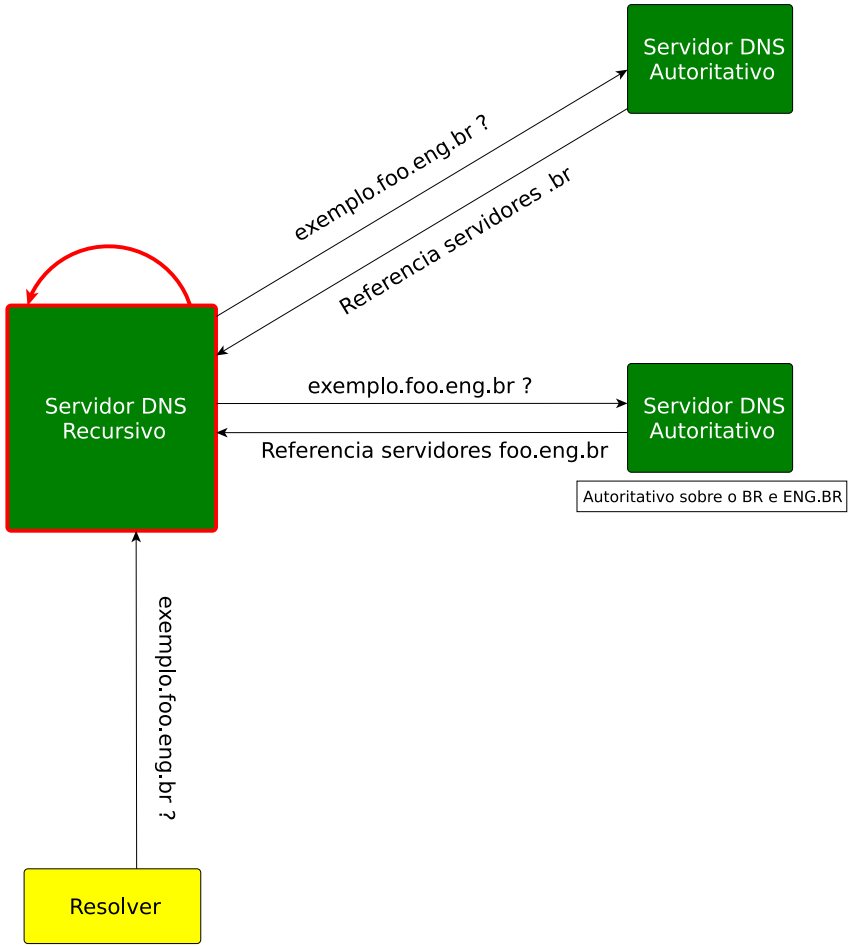
Exemplo



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

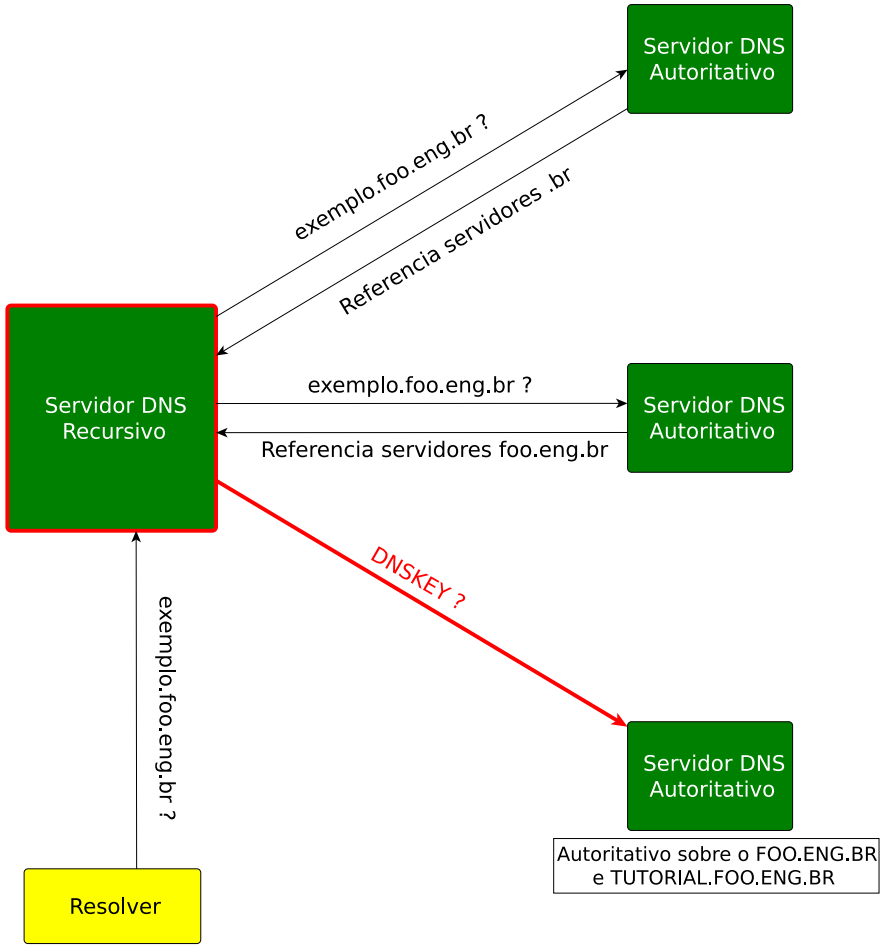
  e com autoridade sobre os Records:
  - DS do "foo.eng.br"
  - RRSIG do Record DS

Exemplo

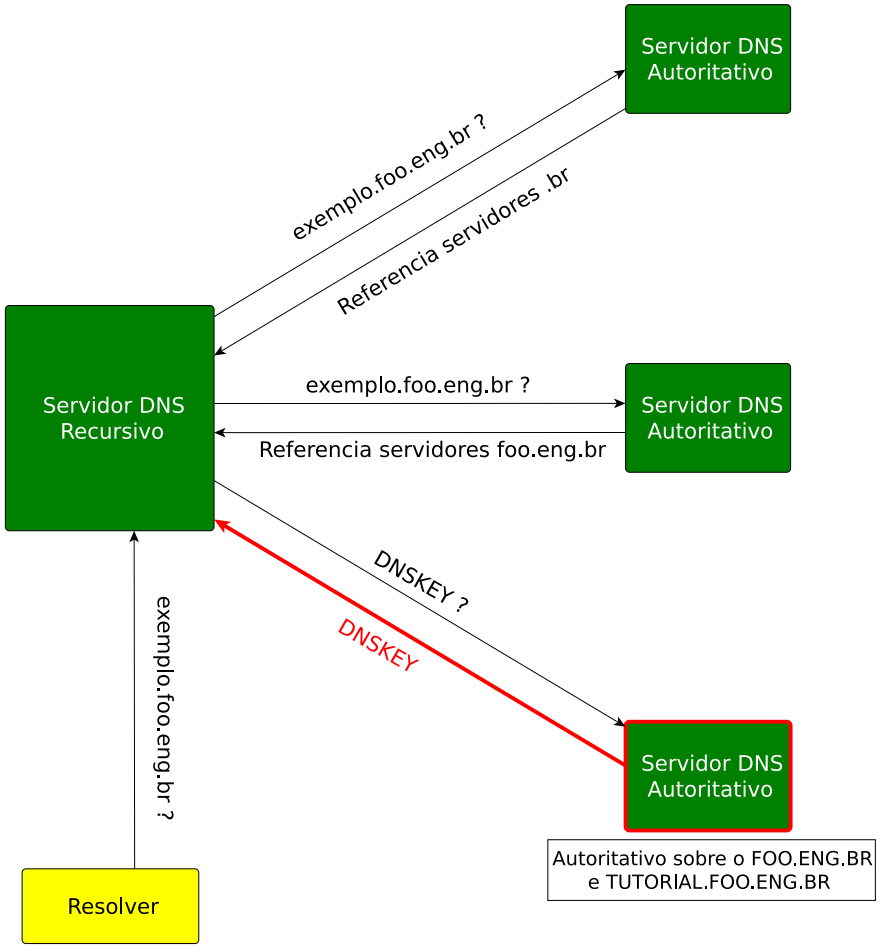


- O servidor DNS recursivo utiliza a DNSKEY para checar a assinatura (RRSIG) do Record DS

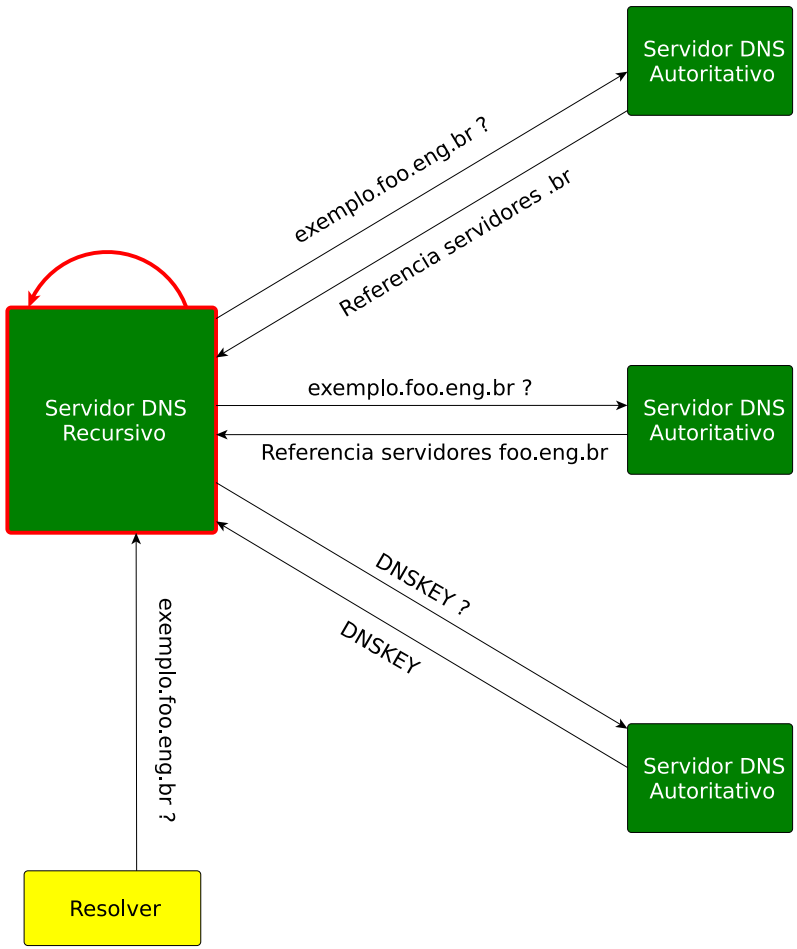
Exemplo


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 TUTORIAL.FOO.ENG.BR
Resolver

Exemplo

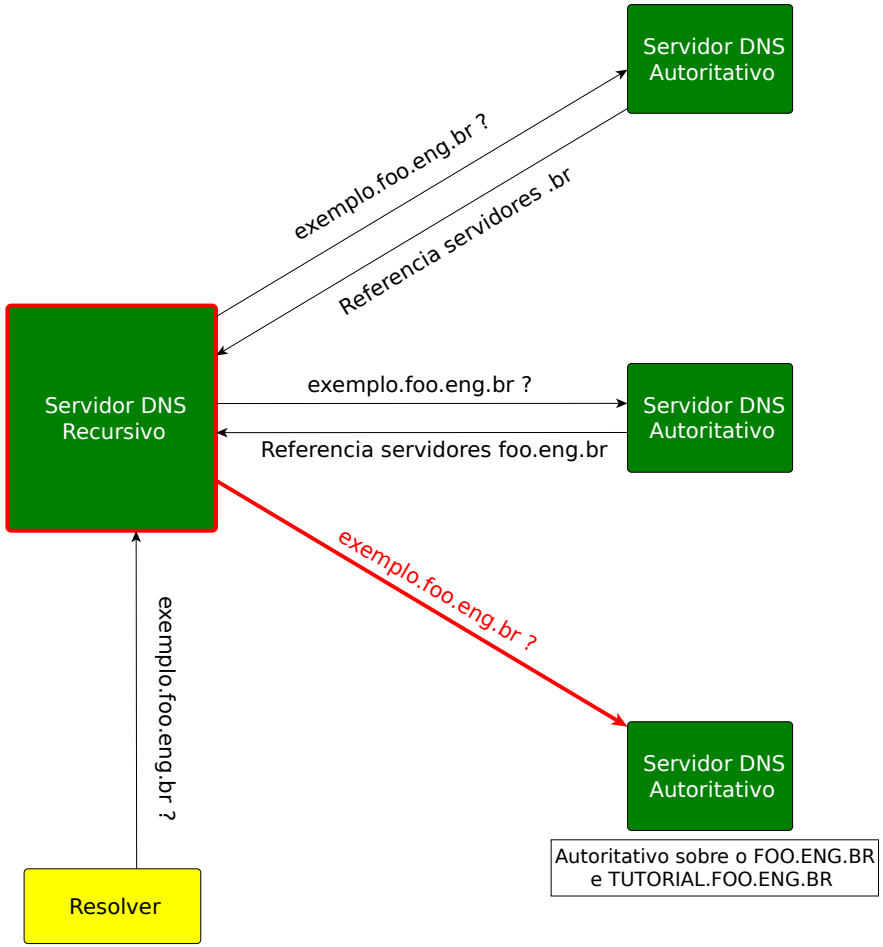

Servidor DNS Autoritativo
exemplo.foo.eng.br ?
Referencia servidores .br
Servidor DNS Recursivo
exemplo.foo.eng.br ?
Servidor DNS Autoritativo
Referencia servidores foo.eng.br
DNSKEY ?
DNSKEY
exemplo.foo.eng.br ?
Servidor DNS Autoritativo
Autoritativo sobre o FOO.ENG.BR e TUTORIAL.FOO.ENG.BR
Resolver

Exemplo



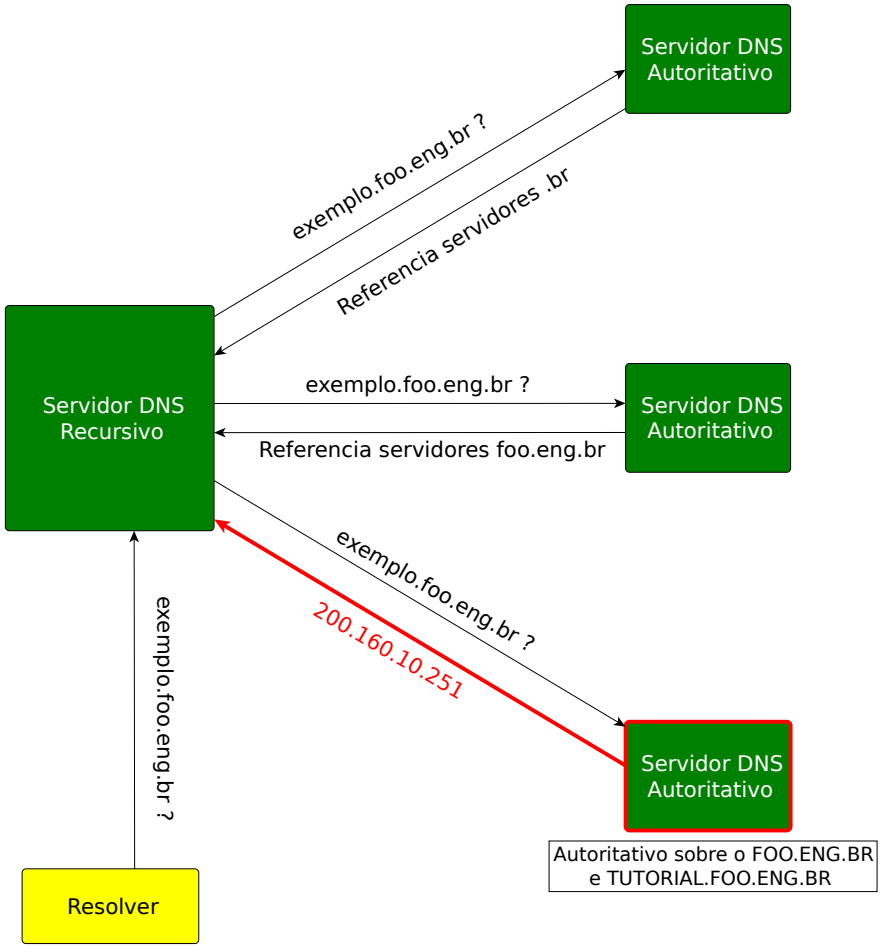
- O servidor DNS recursivo verifica através do DS e da DNSKEY, se este servidor DNS é válido.

Exemplo

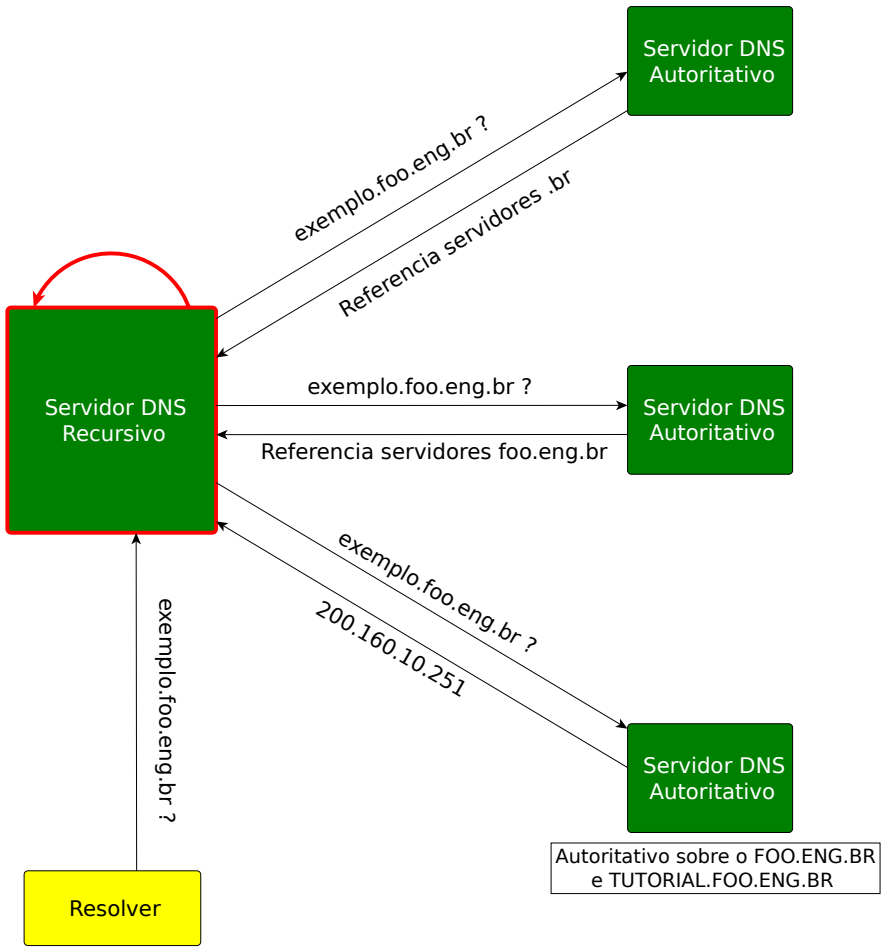

Servidor DNS Autoritativo
exemplo.foo.eng.br ?
Referencia servidores .br
Servidor DNS Recursivo
exemplo.foo.eng.br ?
Servidor DNS Autoritativo
Referencia servidores foo.eng.br
exemplo.foo.eng.br ?
exemplo.foo.eng.br ?
Servidor DNS Autoritativo
Autoritativo sobre o FOO.ENG.BR e TUTORIAL.FOO.ENG.BR
Resolver

Exemplo

- Retorna o Record A e sua assinatura RRSIG.

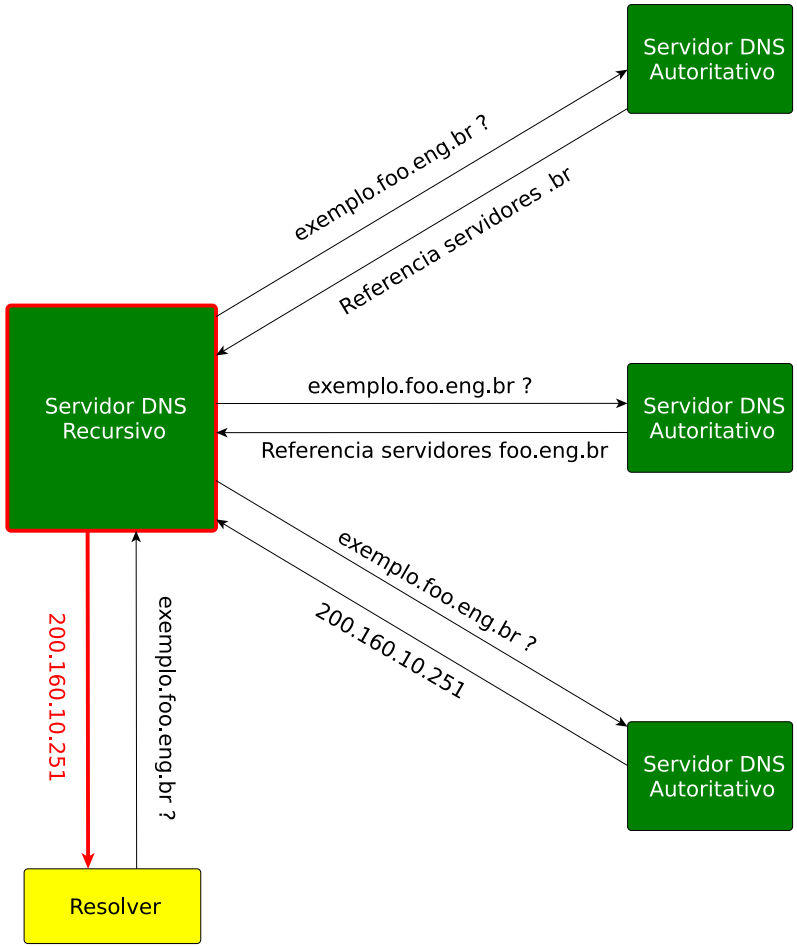


Exemplo



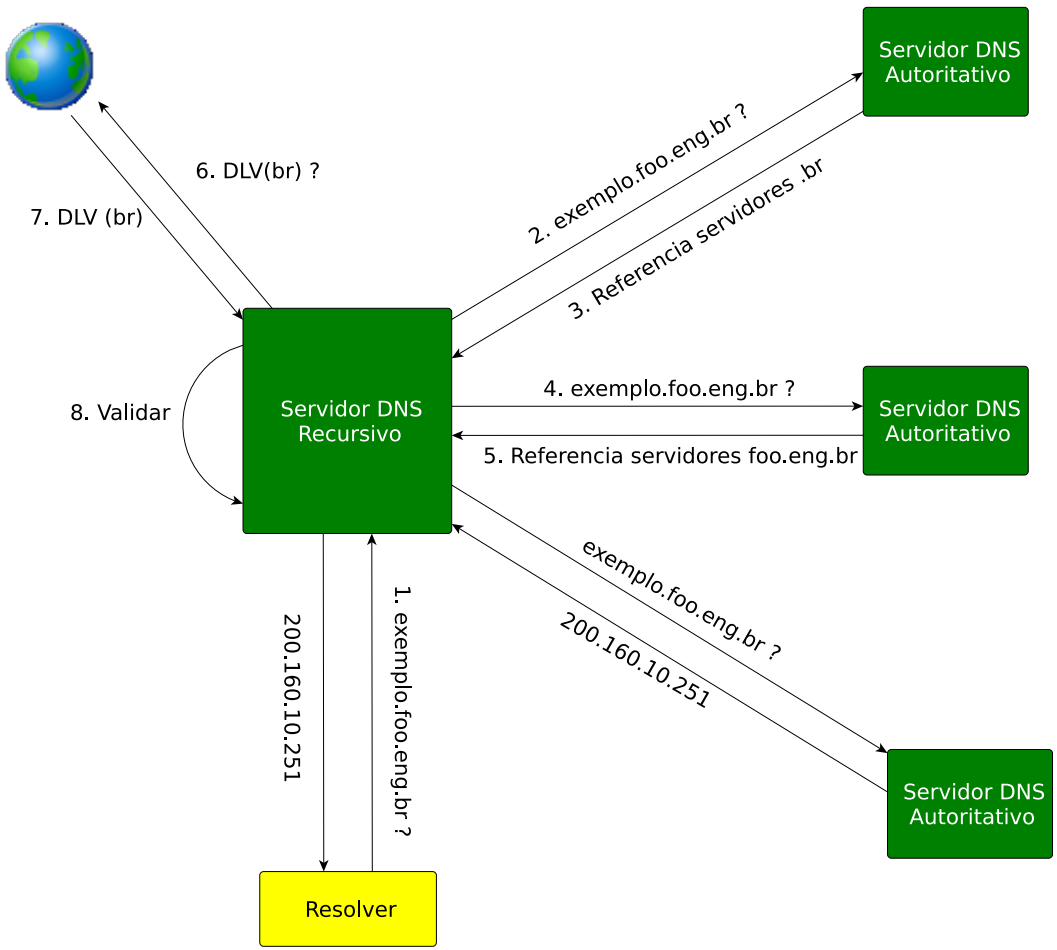
- O servidor DNS recursivo utiliza a DNSKEY para checar a assinatura (RRSIG) do Record A

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

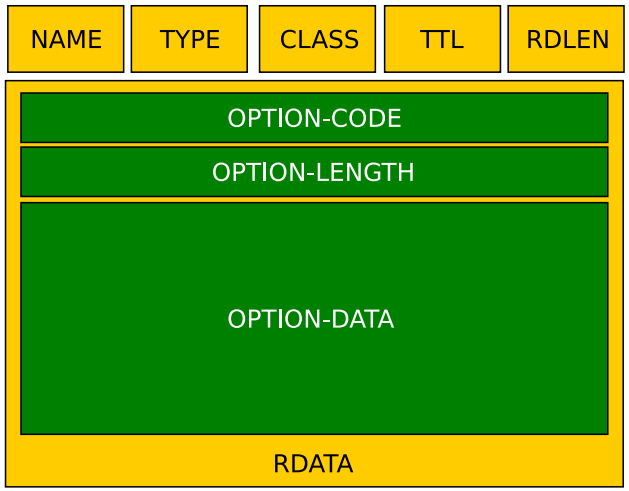
EDNS0 (RFC 2671)

Criado de forma a tornar mais flexíveis as limitações dos campos no protocolo DNS e possibilitar a análise 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 as seguintes opções:

```
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

Conceito de Chaves

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

registro.br
Registro de Domínios para a Internet no Brasil

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

Conceito de Chaves

registro.br
Registro de Domínios para a Internet no Brasil

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 aconselhavél a utilização de somente uma única chave.

Mais informações sobre como proceder no slide 120.

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 à 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

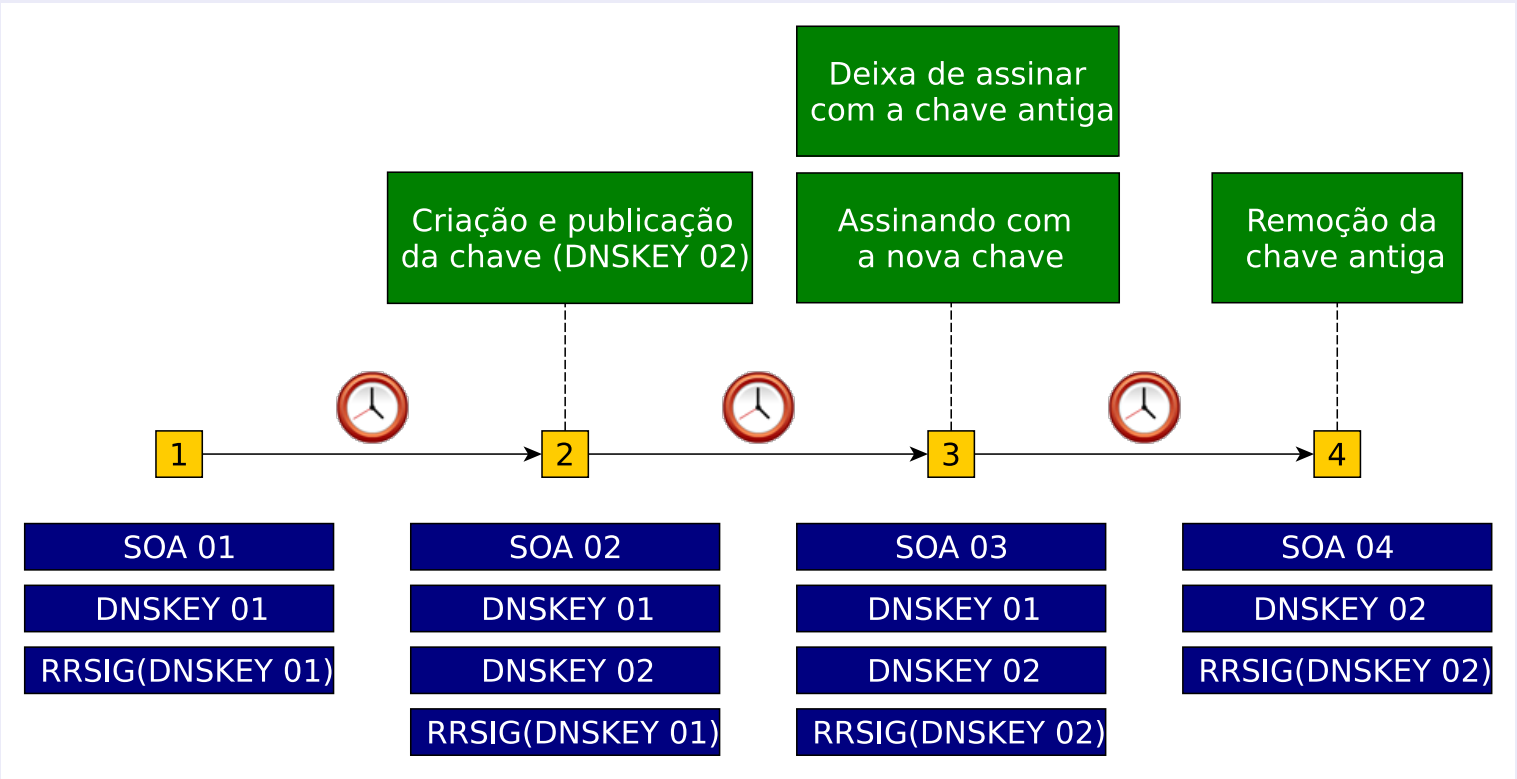
- 2 dias paras os records do APEX (possuem o nome da zona)
- 6 horas para a record DNSKEY
- 1 dia para os demais records

OBS: O record NSEC possuirá o TTL 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

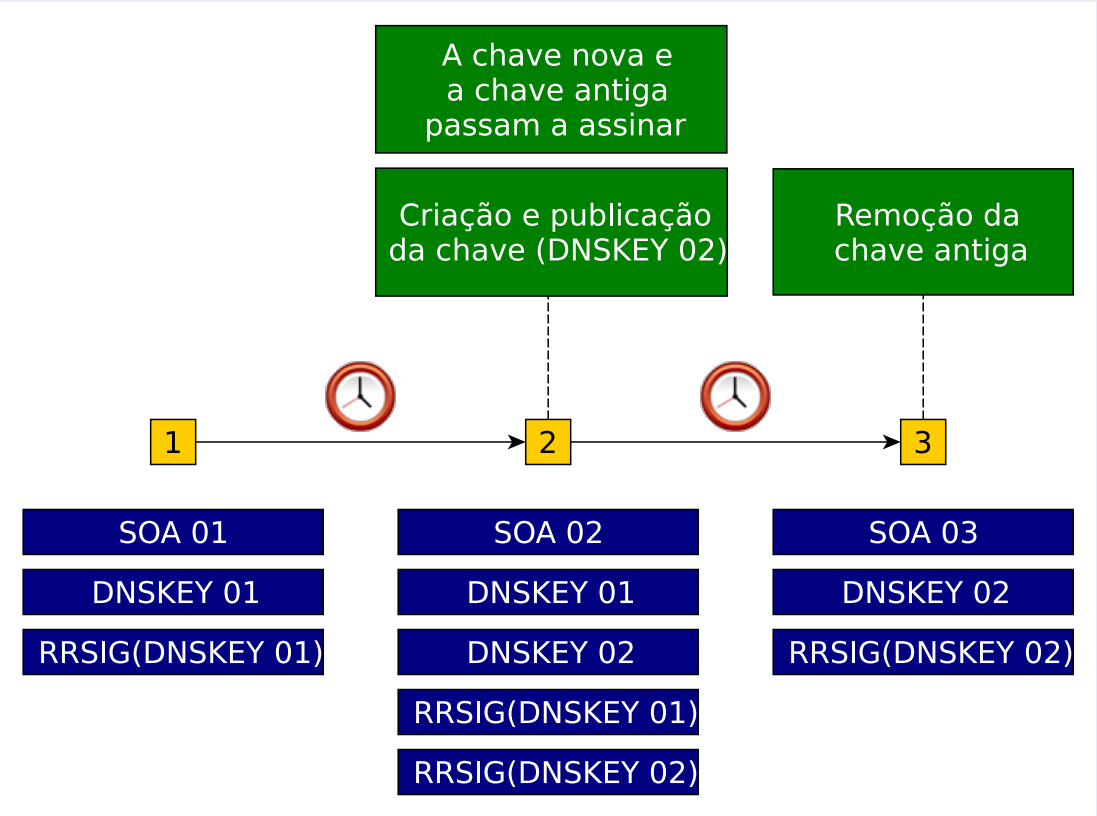
Rollover (Substituição de Chaves - RFC 4641)

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/info/dnssec-policy.html`

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.

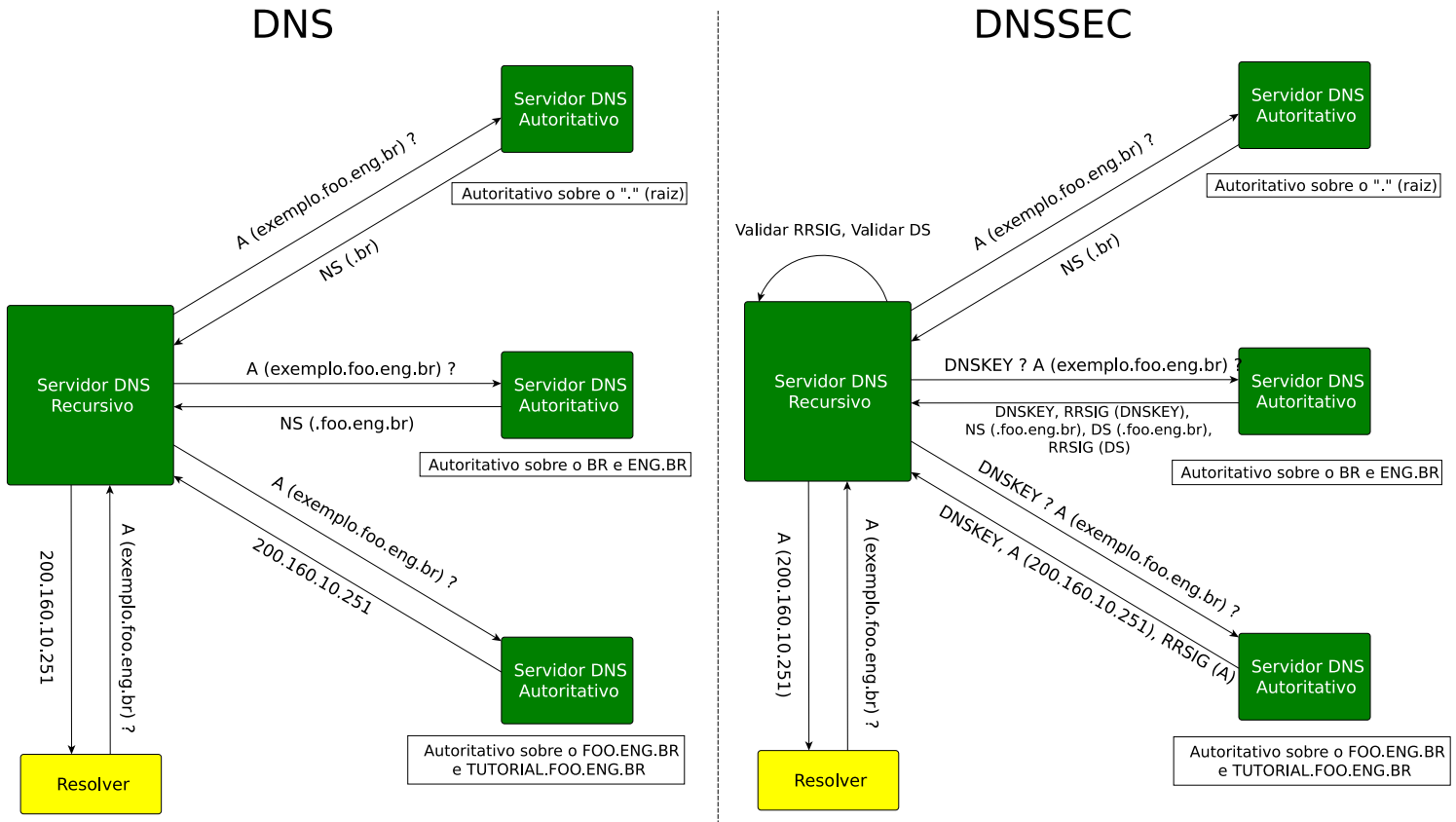
Como o Registro.br tem autoridade sobre o BR e *.BR, não existe necessidade de KSK para *.BR.

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]	NSEC3[c]	TSIG	IPv6
ANS	√			√	√		√	√
BIND	√	√	√	√	√	√[d]	√	√
djbdns	√	√	√					√
DNSSHIM	√				√		√	√
IPControl	√	√	√	√	√		√	√
IPM DNS	√	√	√	√	√		√	√
MaraDNS	√	√	√					?
Microsoft DNS	√	√	√	√	√[e]		√	√
NSD	√			√	√	√	√	√
PowerDNS	√	√	√					√
Unbound		√	√		√	√		√
Vantio		√	√	√	√		√	√
VitalQIP	√	√	√	√	√		?	√

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

[b] Versão atual do protocolo

[c] Servidores recursivos devem(!) ter suporte a NSEC3 para pleno funcionamento com DNSSEC

[d] Suporte a partir da versão 9.6.0

[e] Suporte a partir da versão Windows Server 2008 R2 ou Windows 7

Softwares

Compatibilidade de Servidores DNS com Sistemas Operacionais

	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

	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		

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

– até a versão 1.2.0 da ldns o DRILL **não** tinha suporte a validação de Records CNAME

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

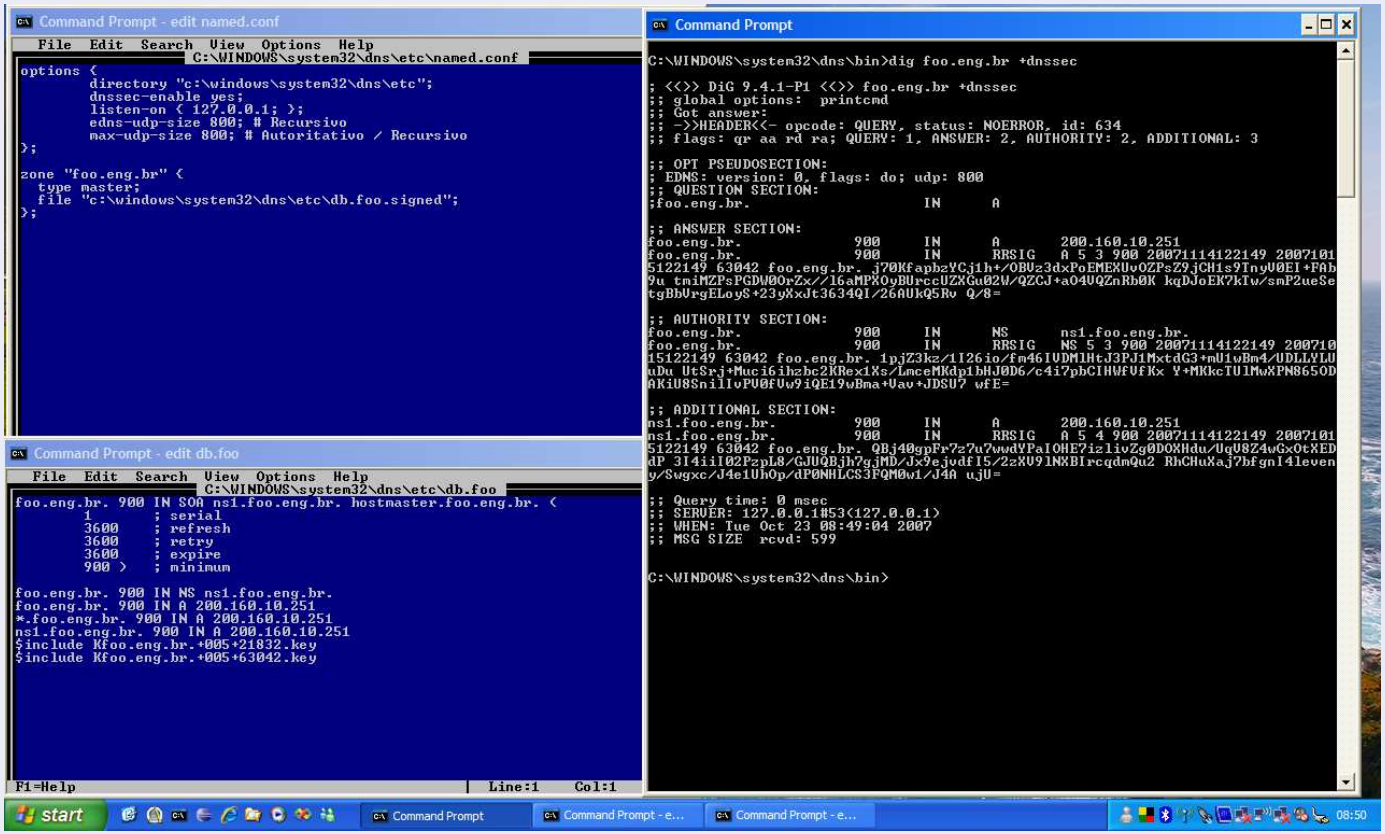
Acesse a propriedade do serviço, e na aba "Log On" selecione a opção "Local System account"

registro.br
Registro de Domínios para a Internet no Brasil

BIND no Windows

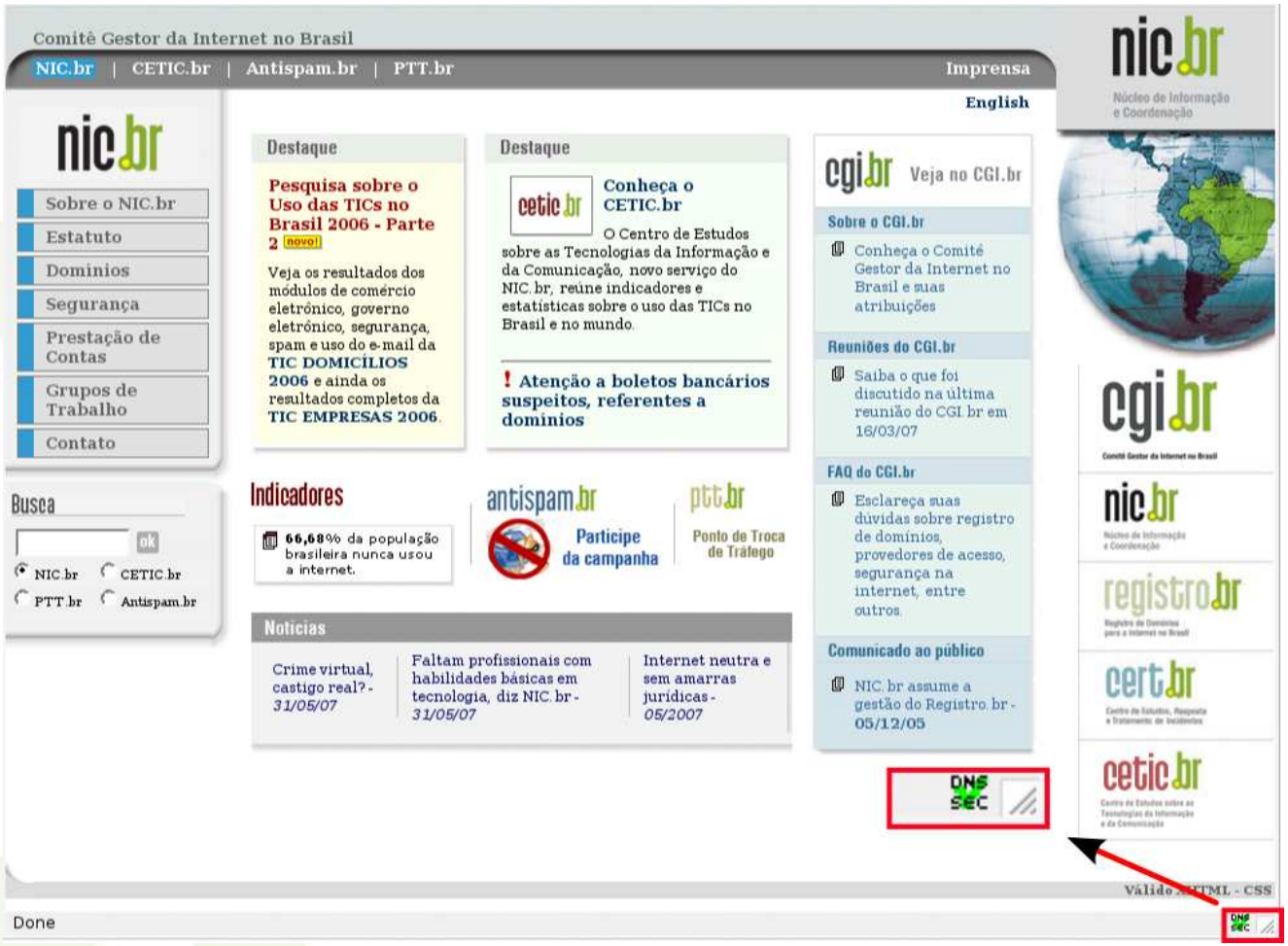
O BIND no Windows funciona da mesma forma que no Linux, sendo que os arquivos ficam localizados em locais diferentes.

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



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

– http://nlnetlabs.nl/projects/drill/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=
```

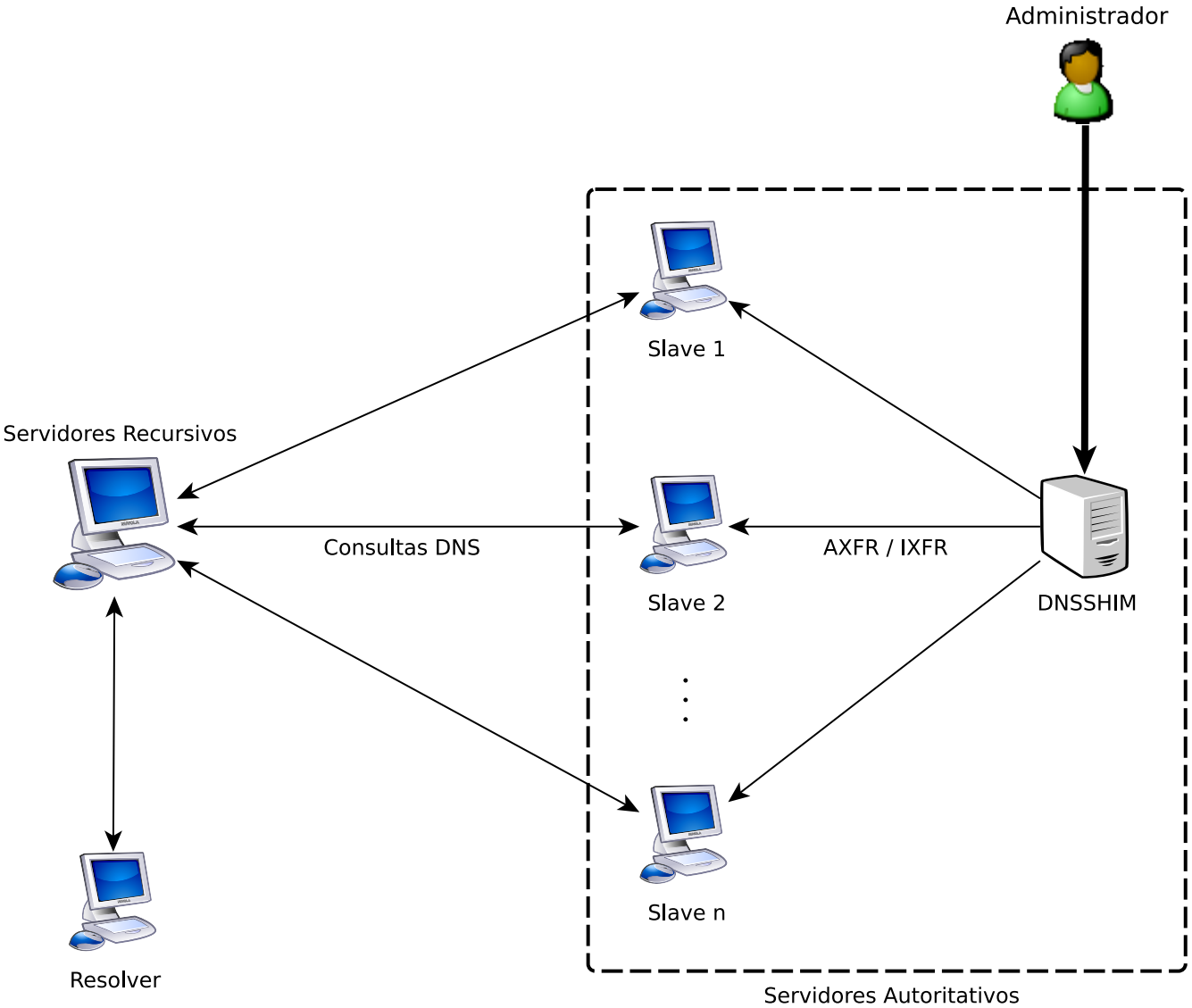
http://registro.br/dnsshim/

- 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

DNSSHIM - DNS Secure Hidden Master



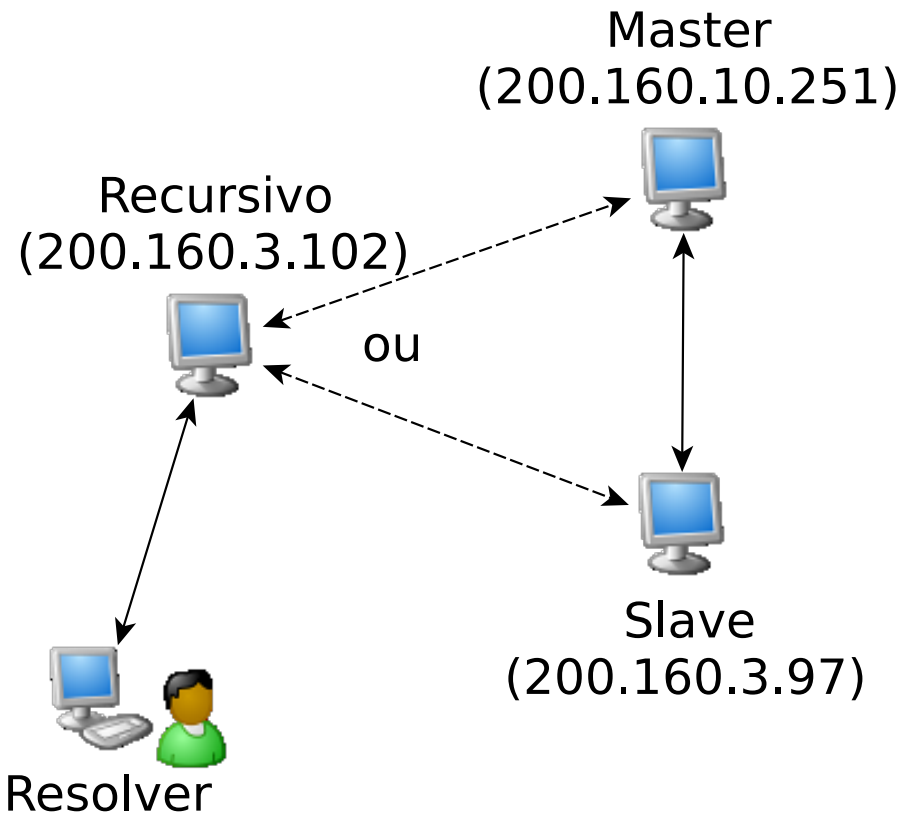
Demonstração prática

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 KSK
   b. Atualização do arquivo de zona
   c. Assinatura da zona
   d. 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 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
foo.eng.br.                IN NS ns1.foo.eng.br.
foo.eng.br.                IN NS ns2.foo.eng.br.
tutorial.foo.eng.br.       IN NS ns2.tutorial.foo.eng.br.
tutorial.foo.eng.br.       IN NS ns1.tutorial.foo.eng.br.
ns1.foo.eng.br.            IN A 200.160.3.97
ns2.foo.eng.br.            IN A 200.160.10.251
ns1.tutorial.foo.eng.br.   IN A 200.160.3.97
ns2.tutorial.foo.eng.br.   IN A 200.160.10.251
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 "tutorial.foo.eng.br" {
    type master;
    file "/etc/namedb/db.tutorial.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 "tutorial.foo.eng.br" {
    type slave;
    file "/etc/namedb/db.tutorial.foo";
    masters {
        200.160.10.251;
    };
};
```

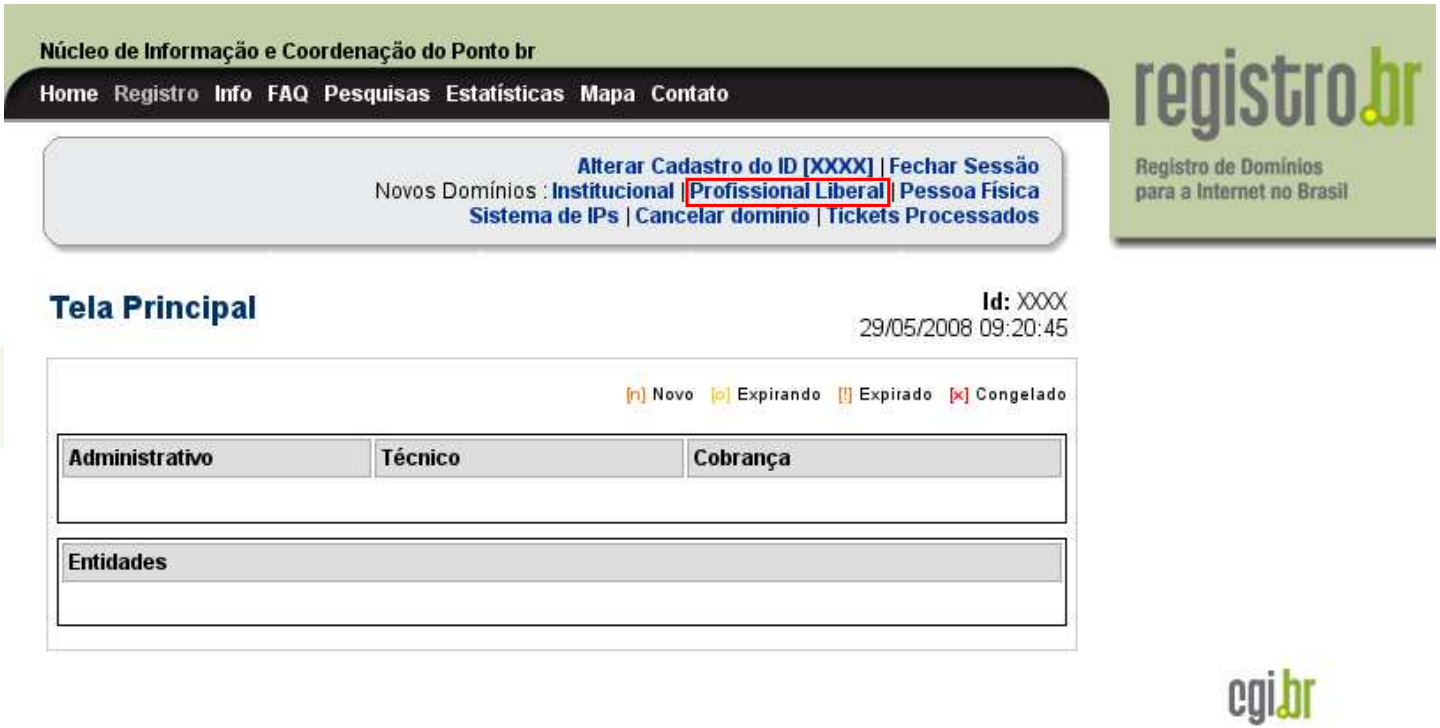
Teste - Consulta de record

Zona foo.eng.br

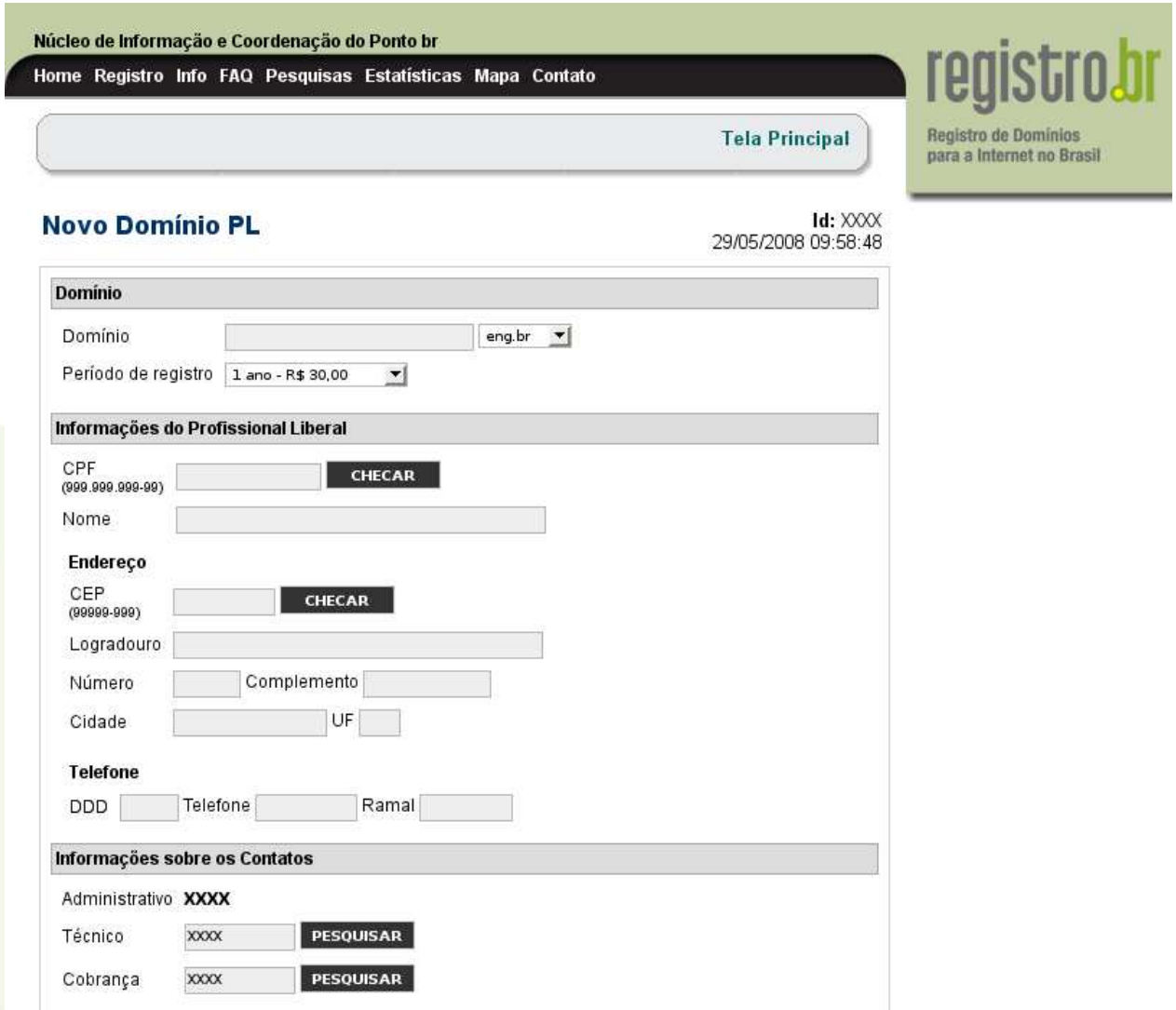
dig @200.160.10.251 foo.eng.br soa +noadditional +multiline

```
; <<>> 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 (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
```

Registro de domínios



Registro de domínios



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
```

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 randomizaçao, como por exemplo: "`-r /dev/urandom`"

OBS1: 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.

Exemplo de Tamanho de chaves

- KSK BR: 1280 bits

Exemplo de arquivos de chaves

Chave pública (.key)

```
foo.eng.br. IN DNSKEY 257 3 5 AwEAAdDaICi4nCQX+dC+kkGlGmi7+Pjww4O5WYZtt+oe1RG329H2+k0Y XhYiZx7tLULD8Fn3DtBC
hGTeFND+gCBj0vFS9MEjxHIkD2gtt3fFIbqN /sQIHDjNGr1M6aFngKxWTENWqkl71hT9jOEvzsLOD+deFDge4sDF5qOQ 4D8njiqIIqDsU
kt3I1cJoFtP9k9RPIijxWdILWuKgh7nEvKpX7eOEuXO YK1W88Av9ctpm3y6lzbsWC0K4OIl7nGTB+qMCbt/ZdYMwcaVuTBHQpEUKNVuq3m
FGj1MxwtadBimmqq+YhleGzn21x0CYmsStwNUAWcb/H9Sqg0G F3CVcH0t86k=
```

Chave privada (.private)

```
Private-key-format:  v1.2
Algorithm:  5 (RSASHA1)
Modulus: 0NogKLicJBf50L6SQaUaaLv4+PDDg7lZhm236h7VEbfb0fb6TRheFiJnHu0tQsPwWfcO0EKEZN4U0P6AIGPS8VL0wSPEciQPaC
23d8Uhuo3+xAgcOM0avUzpoWeArFZMQ1aqSXvWFP2M4S/Ows4P514UOB7iwMXmo5DgPyeOKogioOxSS3cjVwmgW0/2T1E8iKPFZ0gta4qCH
ucS8qlft44S5c5grVbzwC/1y2mbfLqXNuxYLQrg4iXucZMH6owJu39l1gzBxpW5MEdCkRQo1W6reYUaPUzHC1p0GKaaqr5iGV4bOfbXHQJi
axK3A1QBZxv8f1KqDQYXcJVwfS3zqQ==

...
```

Inclusão da chave no arquivo de zona

registro.br
Registro de Domínios para a Internet no Brasil

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
foo.eng.br.                 IN NS ns1.foo.eng.br.
foo.eng.br.                 IN NS ns2.foo.eng.br.
tutorial.foo.eng.br.        IN NS ns1.tutorial.foo.eng.br.
tutorial.foo.eng.br.        IN NS ns2.tutorial.foo.eng.br.
ns1.foo.eng.br.             IN A 200.160.3.97
ns2.foo.eng.br.             IN A 200.160.10.251
ns1.tutorial.foo.eng.br.    IN A 200.160.3.97
ns2.tutorial.foo.eng.br.    IN A 200.160.10.251
exemplo.foo.eng.br.         IN A 200.160.10.251
$include Kfoo.eng.br.+005+62745.key
```

OBS

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

nic.br

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

Onde,

- -z : Ignora o bit SEP da chave KSK e assina toda a zona
- -o : Nome da 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.`

Inclusão dos Records DS das delegações

Caso existam zonas delegadas que utilizem DNSSSEC dentro do seu domínio, os Records DS destas zonas devem ser adicionados no arquivo db.foo de forma a continuar a cadeia de confiança entre o domínio (foo.eng.br) e suas delegações

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 foo.eng.br deve ser re-assinada após incluir o record DS na zona

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; # somente BIND 9.3
    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;
    };
};
```

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://www.isc.org/solutions/dlv`

1. Instalar o BIND, mantendo as configurações padrão
2. No arquivo named.conf, definir "dnssec-enable yes" (somente BIND 9.3) e "dnssec-validation yes" (BIND 9.4 ou superior) 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

Importante - Servidores DNS recursivos com DNSSEC

- Os domínios "com.br" e "org.br" utilizam a extensão NSEC3
- Para validar domínios com DNSSEC - NSEC3 é necessário possuir BIND a partir da versão 9.6.0 ou o Unbound a partir da versão 1.2.0

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; # somente BIND 9.3
    dnssec-validation yes; # BIND 9.4 ou superior
    listen-on { 200.160.3.102; };
};
trusted-keys {
br.                     257 3 5
                        "AwEAAcmqkFULGgm1VlBbUYQEuCzSbEByjAcNInY9gxft
                        bTK+CSYwlGAfxl5hwx7kxOQAZ2ZMLrxD+sTQVC4StoAP
                        PcUhFqEGOV+9GI6SsD/fikQ0IhtXaS6INKkOPOkfBqot
                        k6C5QbbVXcsML54/dtZYWi/Z7CaG2Hz93ouyUMQzIPoh
                        ER+gkbFYq3ewDajqJKNsVm8caT9/mkNw+CQHR+QNmWM=";
};

...
```

Formato da KSK no site do Registro.br

https://registro.br/ksk

A KSK da zona .br é disponibilizada no site Registro.br em diferentes formatos para facilitar sua utilização

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

*DNS RR
br.                             IN DNSKEY 257 3 5 (
                                AwEAAdDoVnG9CyHbPUL2rTnE22uN66gQCrUW5W0NTXJB
                                NmpZXP27w7PMNpyw3XCFQWP/XsT0pdzeEGJ400kdbbPq
                                Xr2lnmEtWMjj3Z/ejR8mZbJ/6OWJQ0k/2YOyo6Tiab1N
                                GbGfs513y6dy1hOFpz+peZzGsCmcaCsTAv+DP/wmm+hN
                                x94QqhVx0bmFUiCVUFKU3TS1GP415eykXvYDjNpy6AM=
                                ) ; key id = 18457

*BIND trusted-keys config
trusted-keys {
br.                         257 3 5
                                "AwEAAdDoVnG9CyHbPUL2rTnE22uN66gQCrUW5W0NTXJB
                                NmpZXP27w7PMNpyw3XCFQWP/XsT0pdzeEGJ400kdbbPq
                                Xr2lnmEtWMjj3Z/ejR8mZbJ/6OWJQ0k/2YOyo6Tiab1N
                                GbGfs513y6dy1hOFpz+peZzGsCmcaCsTAv+DP/wmm+hN
                                x94QqhVx0bmFUiCVUFKU3TS1GP415eykXvYDjNpy6AM=";
};


*UNBOUND trust-anchor config
trust-anchor: "br. DS 18457 5 1 1067149C134A5B5FF8FC5ED0996E4E9E50AC21B1"
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9

iD8DBQFIYsKFu6WbL7zEeNgRApKSAKCvvdSXKWLbgQNW6+ic7B9ZVGB05wCeOjKu
zLAn8366jquYQhv6GBI9+8g=
=ulem
-----END PGP SIGNATURE-----
```

- KSK no formato de record DNS padrão
- KSK no formato do arquivo de configuração do BIND
- KSK no formato do arquivo de configuração do UNBOUND

Ancorando a chave DLV (Recursivo)

1. Obtenha a chave pública do DLV em http://ftp.isc.org/www/dlv/dlv.isc.org.named.conf
2. Inclua a chave pública no bloco trusted-keys no arquivo named.conf
3. Habilite a opção "dnssec-lookaside . trust-anchor dlv.isc.org.;" no bloco options do arquivo named.conf

Exemplo de inclusão de uma chave DLV

```
options {
    ...
    dnssec-enable yes; # somente BIND 9.3
    dnssec-validation yes; # BIND 9.4 ou superior
    dnssec-lookaside .  trust-anchor dlv.isc.org.;
};
trusted-keys {
...
dlv.isc.org.  257 3 5
    "BEAAAAPp1USu3BecNerrrd78zxJIslqFaJ9csRkxd9LCMzvk9Z0wFzoF
    kWAHMmMhWFpSLjPLX8UL6zDg85XE55hzqJKoKJndRqtncUwHkjh6zERN
    uymtKZSCZvkg5mG6Q9YORkcfkQD2GIRxGwx9BW7y3ZhyEf7ht/jEh01N
    ibG/uAhj4qkzBM6mgAhSGuaKdDdo40vMrwdv0CHJ74JYnYqU+vsTxEIw
    c/u+5VdA0+ZOA1+X3yk1qscxHC24ewPoiASE7XlzFqIyuKDlOcFySchT
    Ho/UhNyDra2uAYUH1onUa7ybtdtQclmYVavMplcay4aofVtjU9NqhCtv
    f/dbAtaWguDB";

}; ...
```

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 (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= )
```

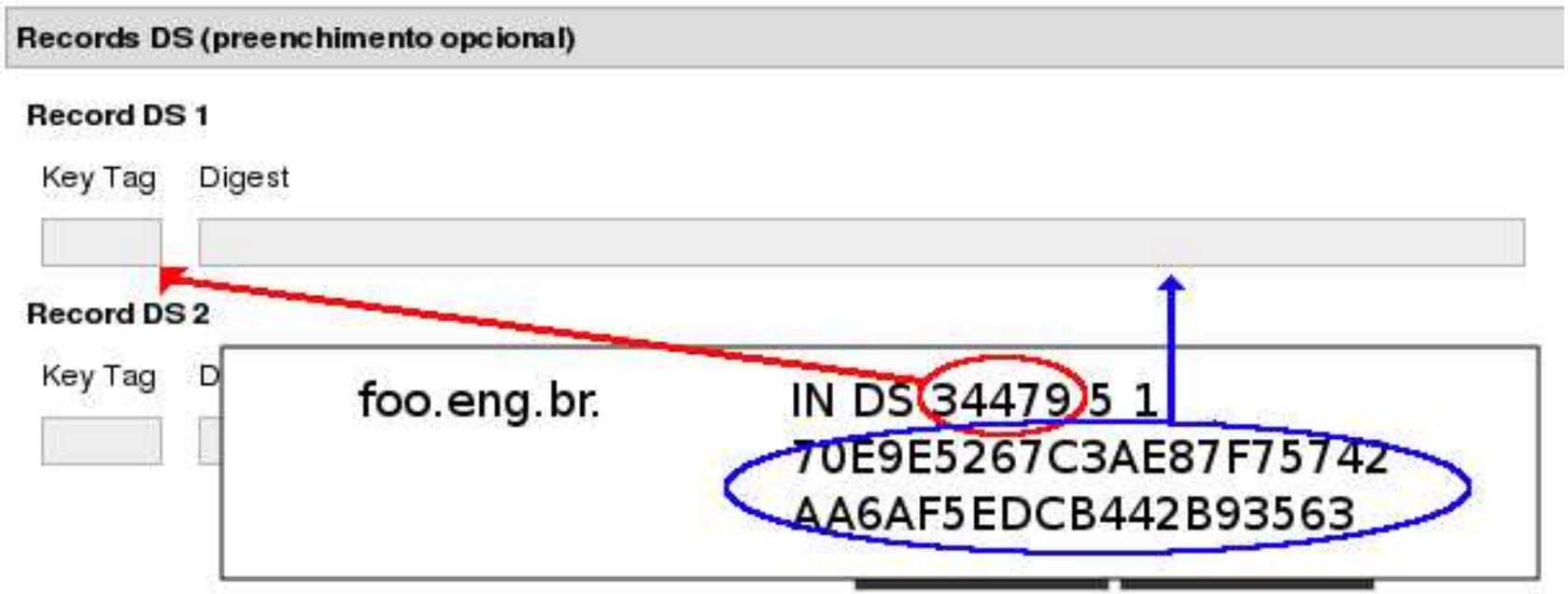
nic.br

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.`



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

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 instalar a biblioteca de desenvolvimento do OPENSSL[a], compilar o BIND 9.4 com a variável de ambiente "`STD_CDEFINES`" definida com o valor "`-DDIG_SIGCHASE=1`" e rodar o comando "configure" com o parametro "–with-openssl"

[a] No Ubuntu o pacote se chama libssl-dev

Ancorando chave para o DIG +sigchase

1. Obter a chave pública da KSK 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

Exemplo de arquivo do DIG

Arquivo trusted-key.key

```
br.                     21600 IN DNSKEY 257 3 5 AwEAAcmqkFULGgm1VlBbUYQEuCzSbEByjAcNInY9gxftbTK+CSYwlGA
fxl5hwx7kxOQAZ2ZMLrxD+sTQVC4StoAPPcUhFqEGOV+9GI6SsD/fikQ0IhtXaS6INKk0POkfBqotk6C5QbbVXcsML54/dtZYWi/Z7CaG2
Hz93ouyUMQzIPohER+gkbFYq3ewDajqJKNsVm8caT9/mkNw+CQHR+QNmWM=
```

KSK do site do Registro.br

```
br.                     21600 IN DNSKEY 257 3 5 (
                                AwEAAcmqkFULGgm1VlBbUYQEuCzSbEByjAcNInY9gxft
                                bTK+CSYwlGAfxl5hwx7kxOQAZ2ZMLrxD+sTQVC4StoAP
                                PcUhFqEGOV+9GI6SsD/fikQ0IhtXaS6INKk0POkfBqot
                                k6C5QbbVXcsML54/dtZYWi/Z7CaG2Hz93ouyUMQzIPoh
                                ER+gkbFYq3ewDajqJKNsVm8caT9/mkNw+CQHR+QNmWM=
                                ) ; key id = 61207
```

Atenção

Existem diferenças entre o formato da KSK no arquivo de configuração do DIG e o formato disponível no site

Teste - Validação da cadeia de confiança

registro.br
Registro de Domínios para a Internet no Brasil

Exemplo

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

```
;; RRset to chase:
foo.eng.br.             83392 IN SOA dixit.foo.eng.br. fneves.registro.br. (
                              2008070301 ; serial
                              3600       ; refresh (1 hour)
                              900        ; retry (15 minutes)
                              3600000    ; expire (5 weeks 6 days 16 hours)
                              3600       ; minimum (1 hour)
                              )
;; RRSIG of the RRset to chase:
foo.eng.br.             83392 IN RRSIG SOA 5 3 86400 20080911163449 (
                              20080703163449 6928 foo.eng.br.
                              i8FmOSkMR6vp9cg4nCfVIPkulspiHlWsW5u8kxCgtL5N
                              TF4ImBks7YHMoEtL8uBux2Y5PiqPXgFnrJebbJJK7m/N
                              XV387mqWOsuUwoTlq/uHDeNNngFsPn1w5AhkxPOZ89wG
                              y5ANukInWzaTYeRk5XzUXvcDqJMeG9BrmQkZPvo= )
Launch a query to find a RRset of type DNSKEY for zone: foo.eng.br.
;; DNSKEYset that signs the RRset to chase:
foo.eng.br.             83392 IN DNSKEY 257 3 5 (
                              AwEAAfhPH7Cg3s1icCNWzAkRU6fQeIHJBibJAoluteAB
                              ZAHnIinvgO6cbFFIP8j+4URgeowBOMUYhAxcCYp1PO1H
                              UhqiL6fGsF649OfW0dR/GF5OBHnlkZdVBVVHQTglXM5a
                              7RsoGHEFKXjSZ/DdwTKA3poJtF61wv0X78UjNxcwhoYF
                              ) ; key id = 6928
```

nic.br

Exemplo (Continuação)

```
;; RRSIG of the DNSKEYset that signs the RRset to chase:
foo.eng.br.             83392 IN RRSIG DNSKEY 5 3 86400 20080911163449 (
                                20080703163449 6928 foo.eng.br.
                                GRc+rmJcsx6OGBsCHcIdAlUXMqTGdIChIW5g0/Ek5V4v
                                8MBIg3mxVSn6dNyByqxjfXt30cew5oyYJU6TaIwXvAL/
                                I8pQpcYprHQwp9uJBoDb/8wLHvkldklmHz/VZCWvHxAz
                                /KDbMnt8RxUwXBMwQMrTBgcjDg2PW7tAgmE21to= )
Launch a query to find a RRset of type DS for zone: foo.eng.br.
;; DSset of the DNSKEYset
foo.eng.br.             18592 IN DS 6928 5 1 (
                                CA7D9EE79CC37D8DC8011F33D330436DF76220D1 )
;; RRSIG of the DSset of the DNSKEYset
foo.eng.br.             18592 IN RRSIG DS 5 3 86400 20080721050001 (
                                20080714050001 33094 eng.br.
                                zQ4S0GiF25+1NTMZh0BT8Aveg4L6SJnyris9jKvBuz7O
                                +rtVkSuGnxHuVHjdoOHj/Ohpsg4xyUFb9tujlonJdtX8
                                qS3RK0C6pD59/q91UBiTI659Px3BK6cZGb7Lvc11lnna
                                /1Xj4t4/RG3L+Ft8PyNl5lFad8/ViPHFnmnsv30= )
```

Teste - Validação da cadeia de confiança

Exemplo (Continuação)

```
;; WE HAVE MATERIAL, WE NOW DO VALIDATION
;; VERIFYING SOA RRset for foo.eng.br. with DNSKEY:6928: 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 foo.eng.br. with DNSKEY:6928: 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: eng.br.
;; DNSKEYset that signs the RRset to chase:
eng.br.   18592 IN DNSKEY 257 3 5 (
    AwEAAc37RO7W/9o86Cx2qwp1uTSXbkag9k0fW977zHxE
    9l6LIKgxq3d8Sj/n4esUpVkRev8HloRqy3l7Yh+K0OmG
    OUiEzfAoYiR6dA6trfy+ogBzXLOC2QqgYZVDmW0xtzX0
    WIvuZQpRvC6xU/lCb4AJxaekGT9iDql7DGZo0ry/T2jl
    ) ; key id = 33094
;; RRSIG of the DNSKEYset that signs the RRset to chase:
eng.br.   18592 IN RRSIG DNSKEY 5 2 21600 20080721050001 (
    20080714050001 33094 eng.br.
    LGSiquTFsPOaU/2o8tRyQEzbmOHuD6jCC7r3Hk5DB61p
    HeDds/JKkaURDf/hWDEjmj/C2JIO7JHojkS171hYCHY1
    P45D6S75Qg9T5Bwx1R3F3KvBfgT7jMlejeuD2nslMB77
    8vp+e2RAjCGJInJ0ugoszZoK7L4a/5VoP+ZLxio= )
Launch a query to find a RRset of type DS for zone: eng.br.
;; DSset of the DNSKEYset
eng.br.   4970 IN DS 33094 5 1 (
    C9B752615F450C0231762D263A8A704BFBEEBABD )
```

Exemplo (Continuação)

```
;; WE HAVE MATERIAL, WE NOW DO VALIDATION
;; RRSIG of the DSset of the DNSKEYset
eng.br.   4970 IN RRSIG DS 5 2 86400 20080721050001 (
    20080714050001 63183 br.
    Ob362cVMBK00WBq2sb6tS9aD6/j7GuJTWSEOg5XDk/SI
    ndP/szpxdZVCcRgPocssmTxt7BIXWLIs0JPqA4YQQSz8
    ZK84SJLQnzVs7J/ruZG4vUsS9/Xy8Ha810d6Y5P5/4BL
    USviI5zPoV41j0HTrVGDblUGnttETsg9+fb+WSsg7Y+/
    9p3UcKPV9n6XxPbW )
;; WE HAVE MATERIAL, WE NOW DO VALIDATION
;; VERIFYING DS RRset for foo.eng.br. with DNSKEY:33094: 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:33094: 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.
;; Truncated, retrying in TCP mode.
;; DNSKEYset that signs the RRset to chase:
br.   18592 IN DNSKEY 257 3 5 (
    AwEAAdDoVnG9CyHbPUL2rTnE22uN66gQCrUW5W0NTXJB
    NmpZXP27w7PMNpyw3XCFQWP/XsT0pdzeEGJ400kdbbPq
    Xr2lnmEtWMjj3Z/ejR8mZbJ/6OWJQ0k/2YOyo6Tiab1N
    GbGfs513y6dy1hOFpz+peZzGsCmcaCsTAv+DP/wmm+hN
    x94QqhVx0bmFUiCVUFKU3TS1GP415eykXvYDjNpy6AM=
    ) ; key id = 18457
```

Exemplo (Continuação)

```
   18592 IN DNSKEY 256 3 5 (
    AwEAAae2jeyarOoqyrNopuBMIJ9zk4JSxQm4f0Mc/InK
    bqqAF268sVb+pZoZScMAyIZADj31w1Xc7F/8qQQ0WWIe
    YpQ8YpsORVqraKiiLiA0+S7GUBbNACebsyK04ESAp3qU
    R63i7jHDIjwBNwvJo/GRMjoNoQlmUgdbKis+wxnGeWgY
    HLOOkPhPXqnfUn8ohvOK9Q==
    ) ; key id = 63183
   18592 IN DNSKEY 257 3 5 (
    AwEAAcmqkFULGgm1VlBbUYQEuCzSbEByjAcNInY9gxft
    bTK+CSYwlGAfxl5hwx7kxOQAZ2ZMLrxD+sTQVC4StoAP
    PcUhFqEGOV+9GI6SsD/fikQ0IhtXaS6INKkOPOkfBqot
    k6C5QbbVXcsML54/dtZYWi/Z7CaG2Hz93ouyUMQzIPoh
    ER+gkbFYq3ewDajqJKNsVm8caT9/mkNw+CQHR+QNmWM=
    ) ; key id = 61207
;; RRSIG of the DNSKEYset that signs the RRset to chase:
br.   18592 IN RRSIG DNSKEY 5 1 21600 20080721050001 (
    20080714050001 63183 br.
    Oyg8s2L+Omqt6hvJqG5ICkaPeJPH/S/+Uub6gOYfcyzo
    rO0bIY4pPL+QzzyQtiVnopR7cb9zF6+3V6h/Z17556LI
    kGfM0vYtFfneD1tLRnJCZpb5CNN0PM1RS7pweaWt0Zmb
    moQy/fmcu615farDUEBXiH690sd6LobVzFg6iarH6DV2
    1tlAahPgHuofW71w )
   18592 IN RRSIG DNSKEY 5 1 21600 20080908000000 (
    20080624173000 18457 br.
    c3pko0teEvAtb2RCkgeOpysWUT4xmCphO+x5rWcYZUwI
    uBOOeDs6BdeIvEeyCAlDvbqQf7cvzsgxzk13QoTJr6Eo
    WdHgBwH+A4HbDm+LyrbBli5zjtCyVGfoYuyUDhTfaNBu
    t9FqBkMvYMifDQmkkBoJCoVQF8u4zfJLpL8Kholn9y4D
    ArjxeVzuoDrPe2WQipP1HACzrd4DU9mG/0qRLA== )
```

Teste - Validação da cadeia de confiança

registro.br
Registro de Domínios para a Internet no Brasil

Exemplo (Continuação)

```
   18592 IN RRSIG DNSKEY 5 1 21600 20080908000000 (
    20080624173000 61207 br.
    Vc6Y6INYvWEb5tUoOiMfVaWrMc18G5CYw2O+HhW32t6X
    7LZ7GZlUlZm4TGcIvYNrwWjUfPpvs1aAP3SaE16UjRZj
    1L3oI9U7yD9ekvnq2HxOudSrIODmXWulRaiBbKIPvcOT
    mEoRN+Z9SUCNdQaLKQ9BoUDUkka8jnEQ5dePyH8tNZ3e
    31SkA/AdRwVuMJi/Hzc+JRB4FKz6mEGhoHVJ6A== )
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:63183: success
;; OK We found DNSKEY (or more) to validate the RRset
;; Ok, find a Trusted Key in the DNSKEY RRset: 61207
;; VERIFYING DNSKEY RRset for br. with DNSKEY:61207: success
;; Ok this DNSKEY is a Trusted Key, DNSSEC validation is ok: SUCCESS
```

nic.br

Roteiro - Configurar um Servidor Autoritativo

registro.br
Registro de Domínios para a Internet no Brasil

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

9. Criar chave KSK (dnssec-keygen) (slide 117)
10. Incluir a chave gerada no arquivo de zona do servidor Master (slide 119)
11. Assinar a zona (dnssec-signzone) (slide 120)
12. Se existir delegações assinadas, incluir no arquivo de zona o DS de cada delegação e reassinar a mesma (slide 121)
13. Atualizar o named.conf do servidor Master de forma a utilizar o arquivo de zona .signed e habilitar DNSSEC-ENABLE (slide 123)
14. Atualizar o named.conf do servidor Slave habilitando DNSSEC-ENABLE (slide 122)
15. Restartar o BIND (named) no servidores Master e Slave
16. Adicionar na interface de provisionamento o DS (localizado no arquivo dsset*) (slide 130)
17. Aguardar nova publicação

nic.br

Roteiro - Configurar um Servidor Recursivo

registro.br
Registro de Domínios para a Internet no Brasil

1. Instalar biblioteca de desenvolvimento do OpenSSL
2. Instalar BIND
3. Obter a trusted-key do site do Registro.br (slide 124)
4. Configurar o arquivo named.conf habilitando DNSSEC-ENABLE e DNSSEC-VALIDATION (slide 125)
5. Incluir a trusted-key no arquivo named.conf (slide 125)
6. Executar o BIND (named)

Recomendação

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

nic.br

Roteiro - Teste da Cadeia de Confiança

1. Instalar BIND com sigchase
2. Obter a trusted-key do site do Registro.br (slide 124)
3. Incluir a trusted-key no arquivo /etc/trusted-key.key
4. Realizar testes no servidor (DIG +sigchase)

registro.br
Registro de Domínios para a Internet no Brasil

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

Servidor Recursivo

Trocar a chave ancorada quando ocorrer um rollover do BR

Perguntas?

Fim da Apresentação

Referências

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.

Exemplo Arquivo Zona

registro.br
Registro de Domínios para a Internet no Brasil

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, ou 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.

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

RFC 5155
DNSSEC Hashed Authenticated Denial of Existence

Referências

- 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/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

Obrigado!