

Tutorial DNSSEC ¹

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

Registro.br

16 de setembro de 2010

¹

versão 1.7.0 (Revision: 6393)

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

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

1 DNS

- Conceitos
- Publicação
- Arquitetura
- Vulnerabilidades

2 DNSSEC

- Conceitos
- Resource Records
- Funcionamento
- DNS Vs DNSSEC

• Softwares

3 Implementação

- Configurações
- DNSSEC com BIND
- Resumo Prático

4 Referências

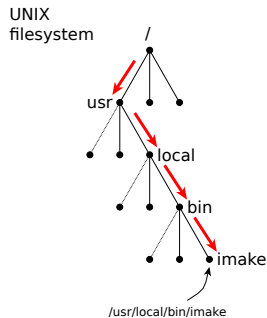
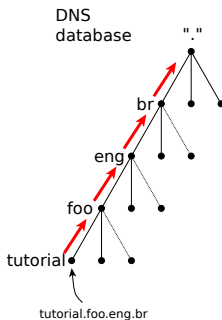
Parte I

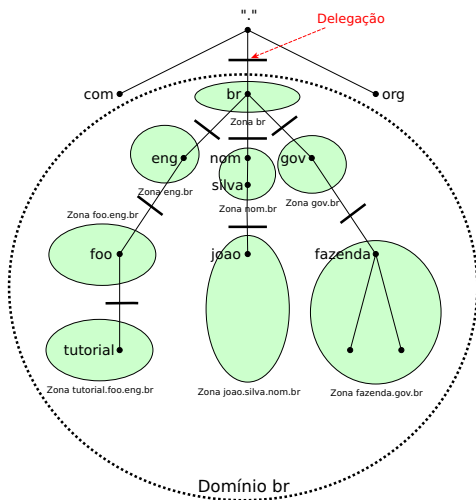
Conceitos de DNS e DNSSEC

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

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

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





Delegação

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

- 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.

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/>

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.



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).

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

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
```

Apêndice I - SOA

```
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
```

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 está vazio ou
sem informações de
br, eng.br,
foo.eng.br,
exemplo.foo.eng.br

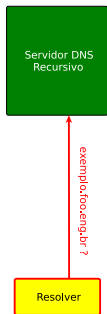
Resolver

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

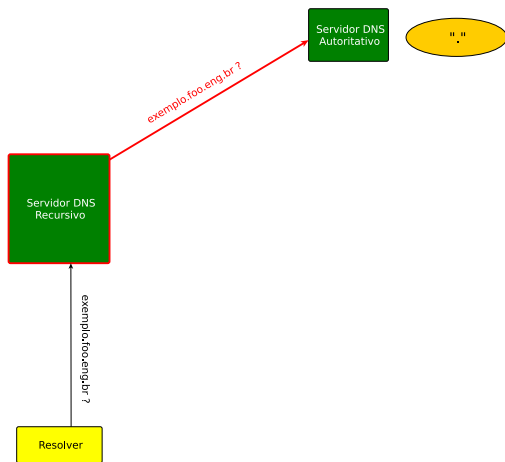
Resolver

Exemplo de requisição de endereço

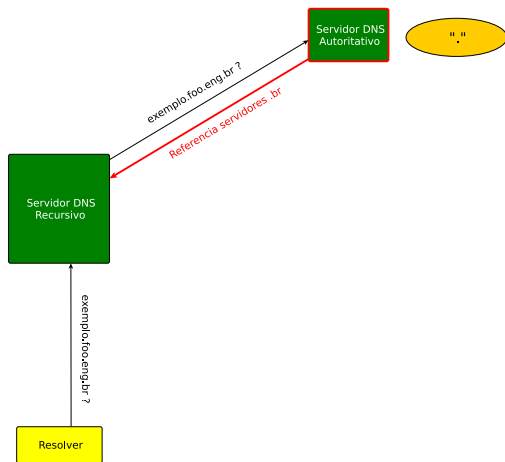
Supondo que o
cache está vazio ou
sem informações de
br, eng.br,
foo.eng.br,
exemplo.foo.eng.br



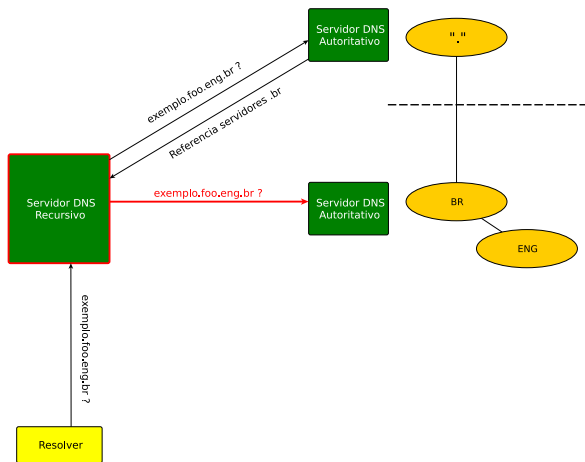
Exemplo de requisição de endereço



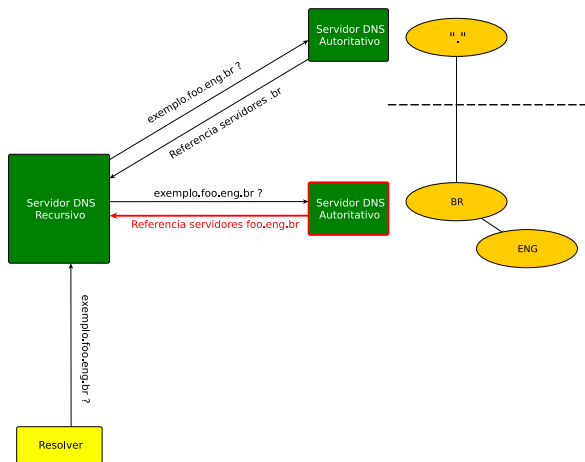
Exemplo de requisição de endereço



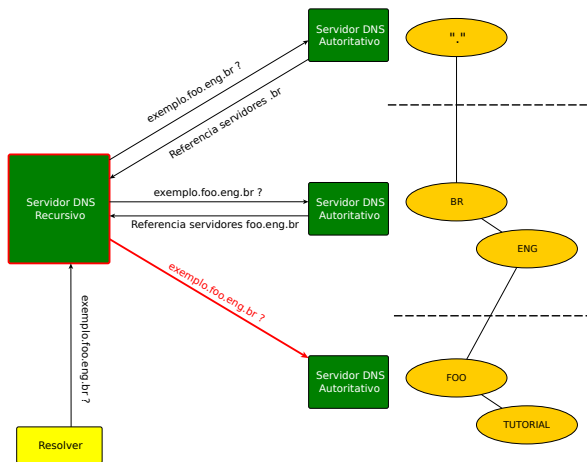
Exemplo de requisição de endereço



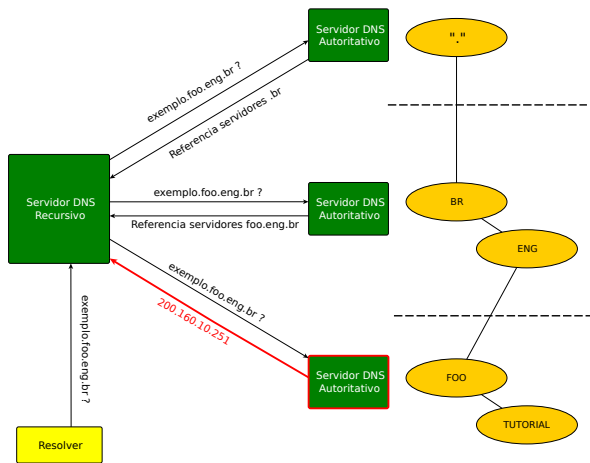
Exemplo de requisição de endereço



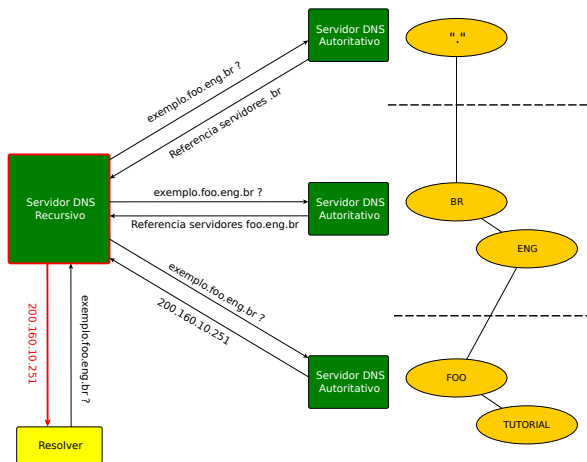
Exemplo de requisição de endereço



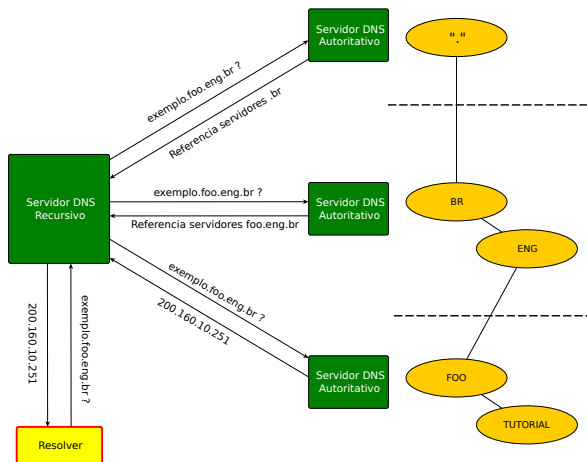
Exemplo de requisição de endereço

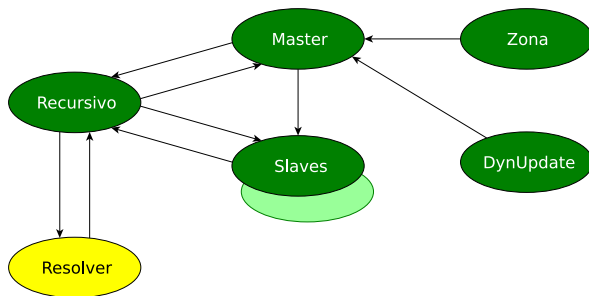


Exemplo de requisição de endereço

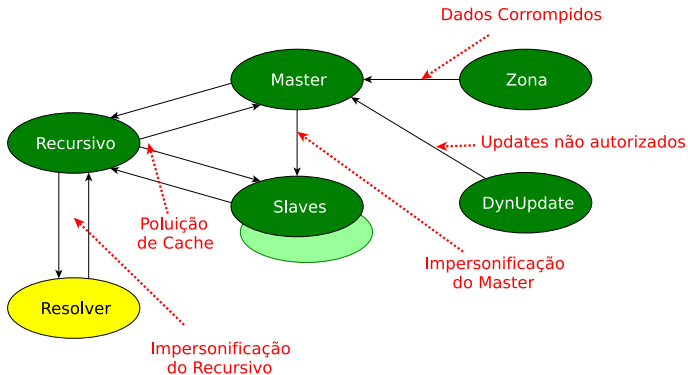


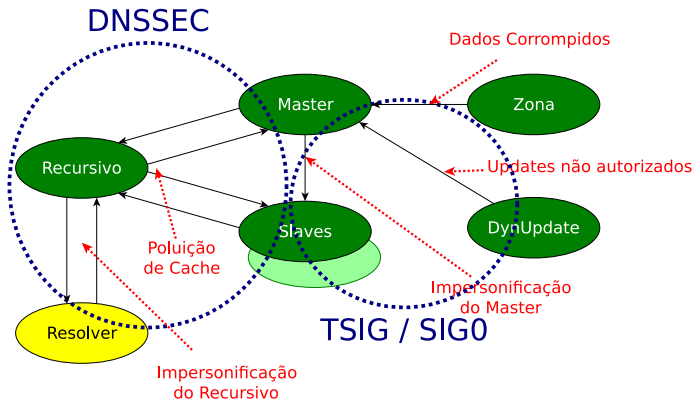
Exemplo de requisição de endereço





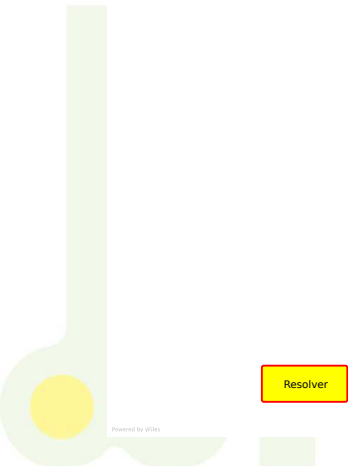
- 1 Resolver faz consultas no Recursivo
- 2 Recursivo faz consultas no Master ou Slave
- 3 Master tem a zona original (via arquivo ou Dynamic Update)
- 4 Slave recebe a zona do Master (AXFR ou IXFR)





Exemplo de Ataque 1

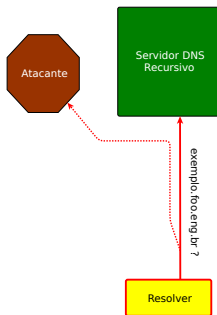
Man-in-The-Middle



Resolver

Exemplo de Ataque 1

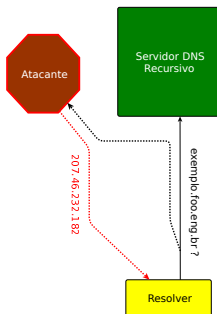
Man-in-The-Middle



Exemplo de Ataque 1

Man-in-The-Middle

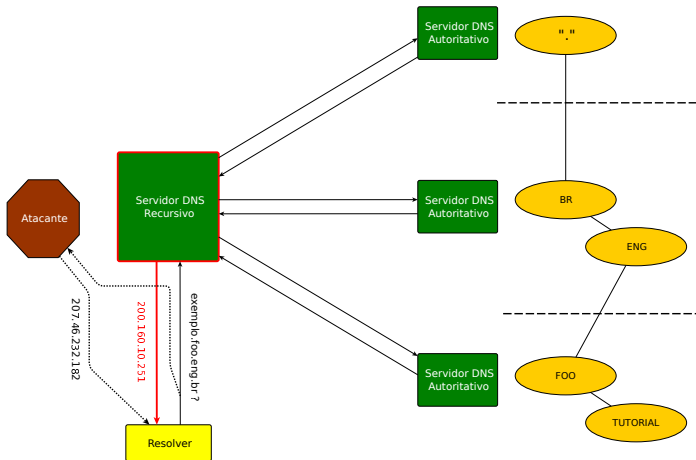
O atacante responde mais rápido, spoofando endereço do recursivo



Exemplo de Ataque 1

Man-in-The-Middle

O atacante responde mais rápido, spoofando endereço do recursivo



Exemplo de Ataque 2

Poluição de Cache

registro.br

Registro de Domínios
para a Internet no Brasil

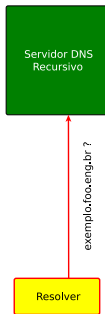


Resolver

nic.br

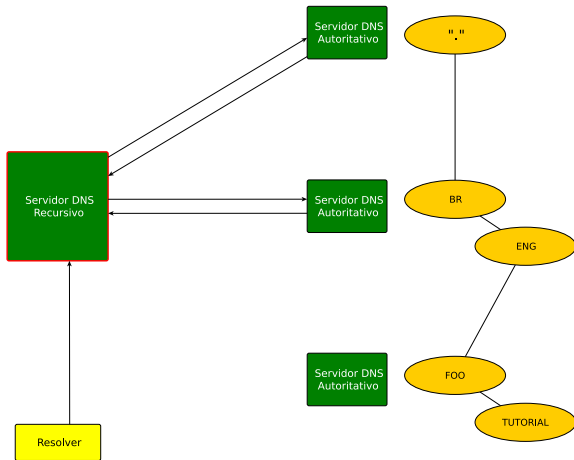
Exemplo de Ataque 2

Poluição de Cache



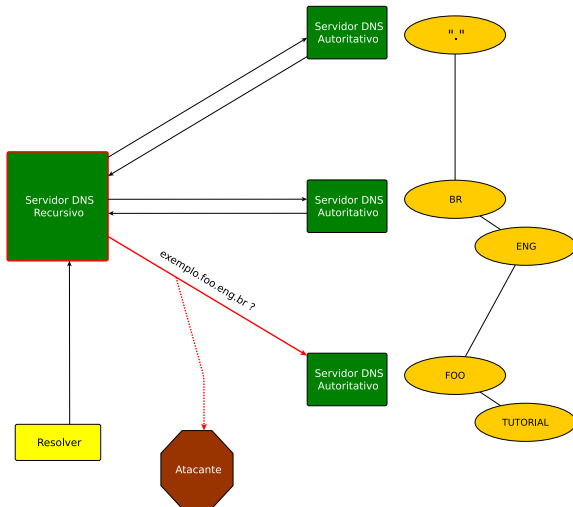
Exemplo de Ataque 2

Poluição de Cache



Exemplo de Ataque 2

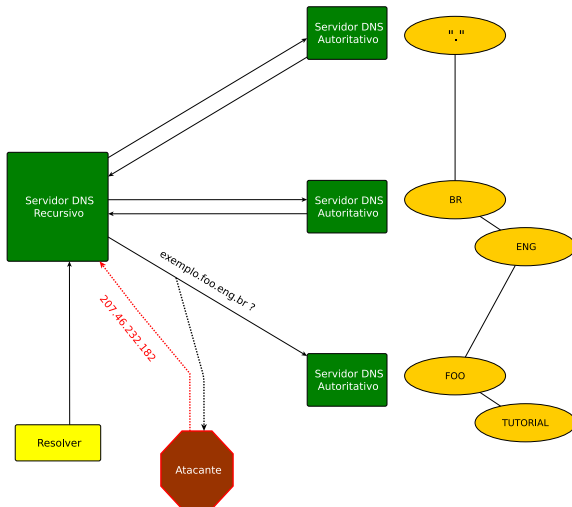
Poluição de Cache



Exemplo de Ataque 2

Poluição de Cache

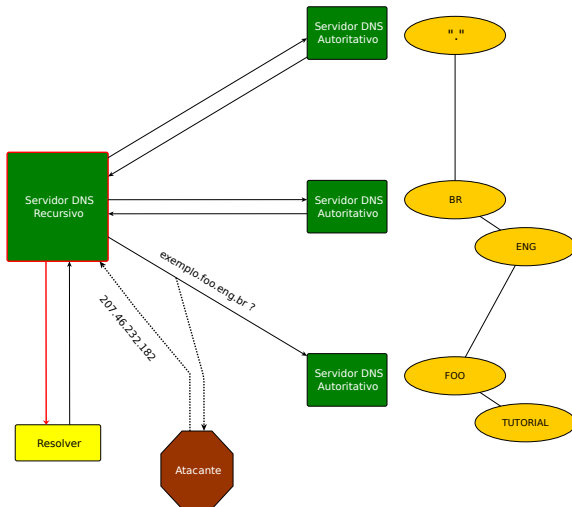
O atacante responde mais rápido, spoofando endereço do autoritativo



Exemplo de Ataque 2

Poluição de Cache

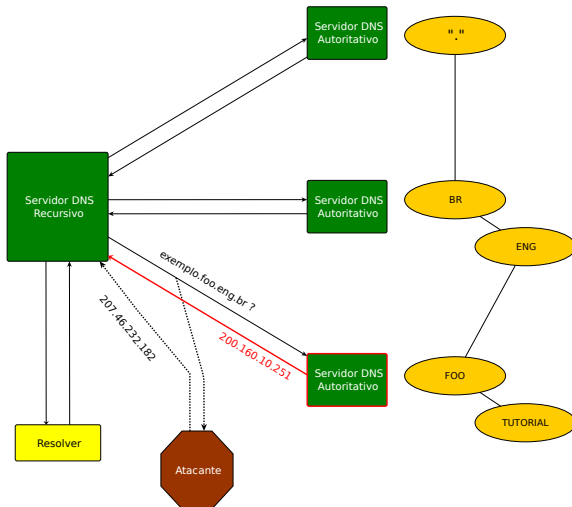
O atacante responde mais rápido, spoofando endereço do autoritativo



Exemplo de Ataque 2

Poluição de Cache

O atacante responde mais rápido, spoofando endereço do autoritativo



Segmentos compartilhados L2 ponto-multiponto

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

Segmentos compartilhados L2 ponto-multiponto

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

Atenção muito cuidado em conferências !

TSIG

Transaction Signatures – RFC 2845

- 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

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...)

Domain Name System **SEC**urity extensions

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

O que garante?

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

O que garante?

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

O que NÃO garante?

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

World Wide DNSSEC Deployment

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



This map was created by Paul Wouters

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>

Quem pode utilizar DNSSEC abaixo do .br?

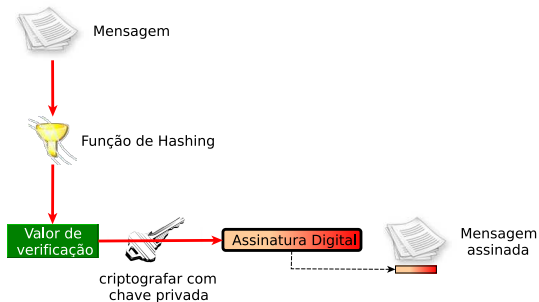
Todos os domínios abaixo do .br podem (e devem) utilizar DNSSEC.

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

Onde DNSSEC é Obrigatório?

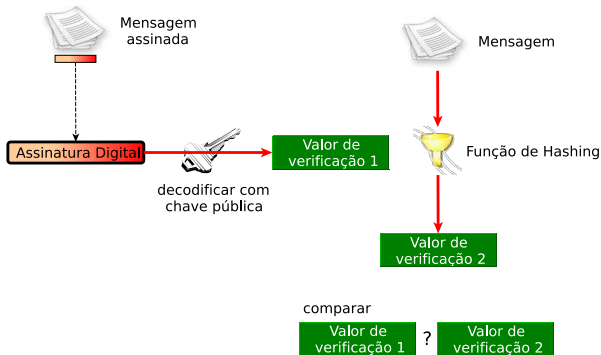
É obrigatório nos registros que estiverem diretamente abaixo dos domínios .B.BR e .JUS.BR

Assinatura



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

Verificação



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

DNSKEY Chave pública

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

É um resource record que armazena a chave pública da zona

```

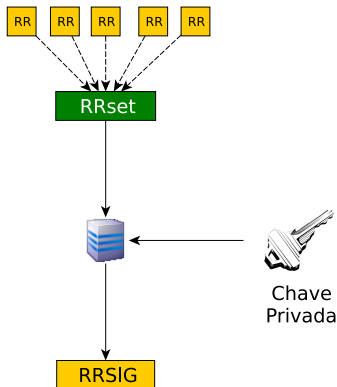
                                1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 3 3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                               | Protocol | Algorithm |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
/                               /
/                               /
/                               /
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
  
```

Exemplo

```

foo.eng.br.      900 IN DNSKEY 256 3 5 (
                  AwEAAeZPN2yMs9q6kgYjFUblEwjCnWwCpQ+TGcJrD5ga
                  XXAbP5MAqIkgZ5J4TU1mmpL1A8gMfd/wUmBkVipXR8FK
                  HRajBZSRfgeKnKaQtrxNZ32Ccts2F6Ylv9WaLXtiqebg
                  OZtuJFpQr6pnIt/FoOI+I7BUSNrX28VTq4jXu/qTrmM/
                  ) ; key id = 62745
  
```

- 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
```

```

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

```

Exemplo

```

foo.eng.br.      900 IN RRSIG SOA 5 3 900 20070617200428 (
                  20070518200428 62745 foo.eng.br.
                  glEeCYyd/CCBfzH64yORAQf90xYDsI4xuBNaam+8DZQZ
                  xeoSLQEetwmp6wBtQ7G10wSM9nEjRRhbZdNPNKJMp2PE
                  lLLgLI+BLwdlz0t8MypcpL0aTm9rc7pP7UR5XLzU1k8D
                  m6ePW1bNkId7i0IPShyoHM7tPVdL2GW51hCujA= )

```

É um hash do Record DNSKEY

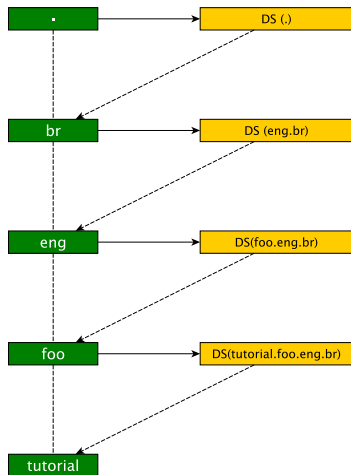
Serve para informar que existe uma cadeia de confiança entre um domínio e seus sub-domínios.

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


```

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

```

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
```

Permite autenticar uma resposta negativa

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

```

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

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.

● Respostas **NXDOMAIN**

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

```
$ dig @200.160.10.251 zzz.foo.eng.br SOA +dnssec
;; ->>HEADER<- opcode: QUERY, status: NXDOMAIN, id: 18301
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1
;; QUESTION SECTION:
;zzz.foo.eng.br.      IN      SOA
;; AUTHORITY SECTION:
foo.eng.br.          0       IN      SOA      ns1.foo.eng.br. hostmaster.foo.eng.br. 1 3600 3600 3600 900
foo.eng.br.          0       IN      RRSIG     SOA 5 3 900 20070617200428 20070518200428 62745 foo.eng.br.
                        glEeCYyd/CCBfzH64yORAQf90xYDsI4xuBNaam+8DZQZxoeSLQEetwmp
                        6wBtQ7G10wSM9nEjRRhbZdNPNKJmp2PElLLgLI+BLwdlZ0t8MypcpL0a
                        Tm9rc7pP7UR5XLzU1k8Dm6ePW1bNkId7i0IPsghyoHM7tPVdL2GW51hCujA=
foo.eng.br.          900     IN      NSEC      ns1.exemplo.foo.eng.br. NS SOA RRSIG NSEC DNSKEY
foo.eng.br.          900     IN      RRSIG     NSEC 5 3 900 20070617200428 20070518200428 62745 foo.eng.br.
                        OCOcPFW5fR6MPHVBaUWfrP9pkIqVc+NDORi6PRwIX/pIdLmAT7NF5Rkc
                        9IfbAHZTxefoqTKqN/vPl1PqSxUzhOrl+atHblaH6yt79CTkmStota7C
                        SLYYXX5c7D93hRYJ2yk1C0xQz6GG9SIp/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/L9fhz0EPYtYGFyMF4gZ1/mxwY31UmX6xVZZPYFJ7x5Kw2uTSD49FK
                        VsdUOLBCAHZ088byAm8EwLe3l+U0/q8RvPimAfpouoivUDcuWtKxs0CzLyc=
```

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

```
$ dig @200.160.10.251 foo.eng.br TXT +dnssec
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60466
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1
;; QUESTION SECTION:
;foo.eng.br.          IN      TXT
;; AUTHORITY SECTION:
foo.eng.br.  900  IN      SOA      ns1.foo.eng.br. hostmaster.foo.eng.br. 1 3600 3600 3600 900
foo.eng.br.  900  IN      RRSIG    SOA 5 3 900 20070617200428 20070518200428 62745 foo.eng.br.
                glEeCYyd/CCBfzH64yORAQf90xYDsI4xuBNaam+8DZQZxoeSLQEetwmp
                6wBtQ7G10wSM9nEjRRhbZdNPNKJMp2PElLLgLI+BLwdlZ0t8MypcpL0a
                Tm9rc7pP7UR5XLzU1k8Dm6ePW1bNkId7i0IPSGhyoHM7tPVdL2GW51hCujA=
foo.eng.br.  900  IN      NSEC    ns1.exemplo.foo.eng.br. NS SOA RRSIG NSEC DNSKEY
foo.eng.br.  900  IN      RRSIG    NSEC 5 3 900 20070617200428 20070518200428 62745 foo.eng.br.
                OCOCpFW5fR6MPhVBaUWfrP9pkIqVc+NDORi6PrwIX/pidLmAT7NF5Rkc
                9IfbAHZTxefoqTKqN/vPl1PqSxUzhOrl+atHb1aH6yt79CTkmStota7C
                SLYYXX5c7D93hRYJ2yk1C0xQz6GG9SIp/U4qR4//TcQDHpqQ4bFs42ZsD4I=
```

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/CCBfzh64yORAQf90xYDsI4xuBNaam+8DZQZxeoSLQEetwmp
                    6wBtQ7G10wSM9nEjRRhbZdNPNKJMp2PElLLgLI+BLwdlz0t8MypcpL0a
                    Tm9rc7p7UR5XLzU1k8Dm6ePW1bNkId7i0IPSghyoHM7tPVdL2GW51hCujA=
;; 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+UeqYkOxgQGQXkBzcKiKQRPwe+1JZlpjEzjU1Uj0HU0Hefa
                    jXzMv7F1FMWYeU51Ybg49HFe67XQV1K54GeAFXWB7YS59yODL0NEBxQ1
                    9QEY6g/00nLpuKTrST8qqd5Fc/eYqN/Ag3GnfcAviZgiQhveGH9mJHWZyc=
```

- 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

- 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

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

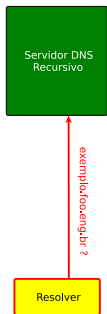
Sempre que utilizar um Servidor Recursivo com DNSSEC habilitado é necessário ancorar a chave pública.

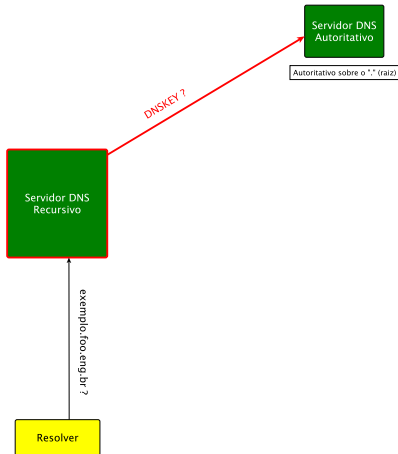
Isto serve para associar o início da cadeia de confiança a um ponto seguro.

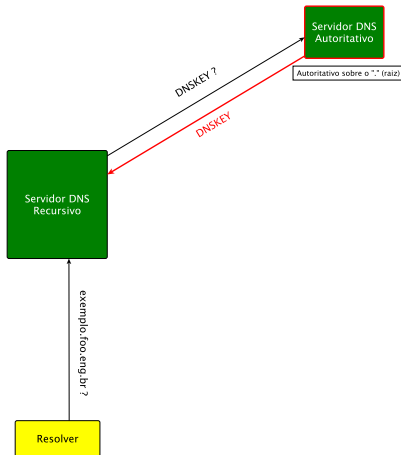
Obtendo a chave a ser ancorada da zona “.” (raiz)

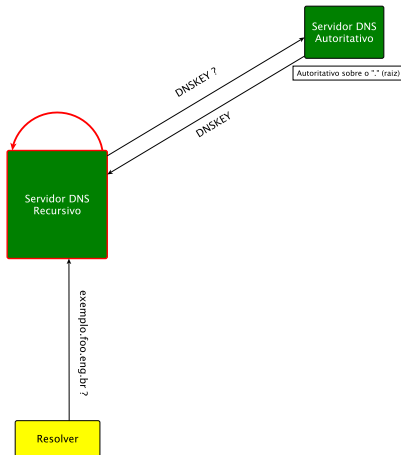
- <https://data.iana.org/root-anchors/>

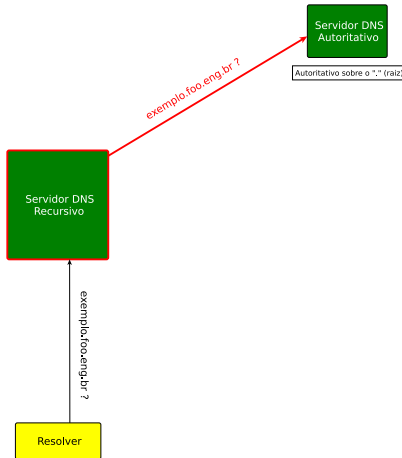
- O resolver recursivo já possui a chave pública da zona "." (raiz) ancorada

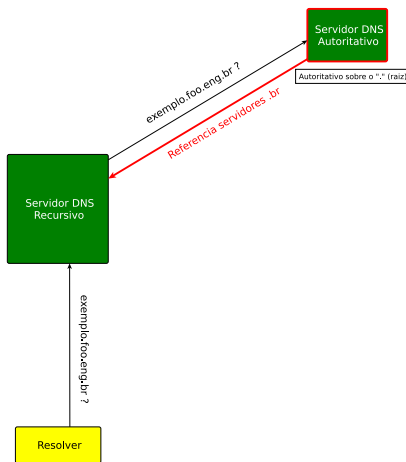


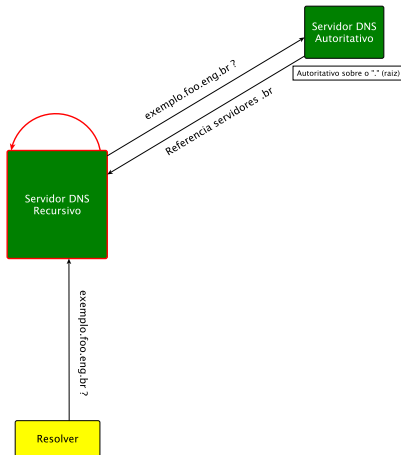


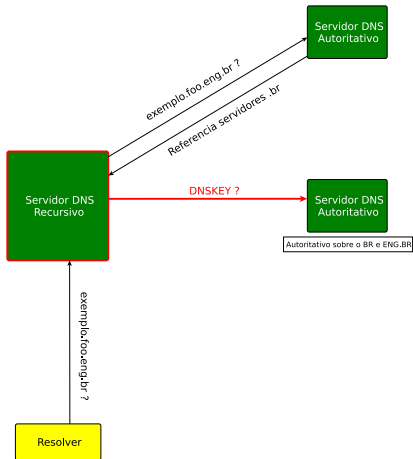




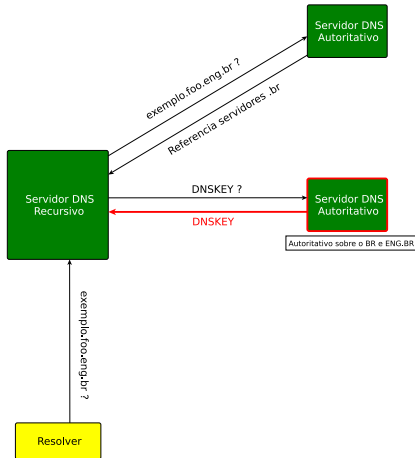


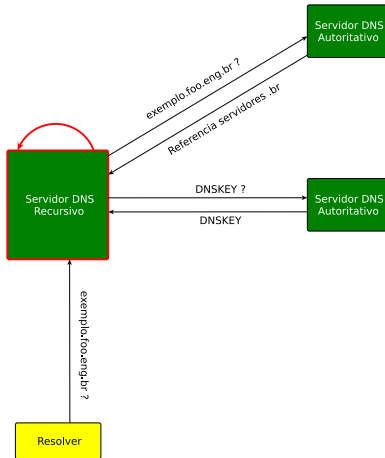




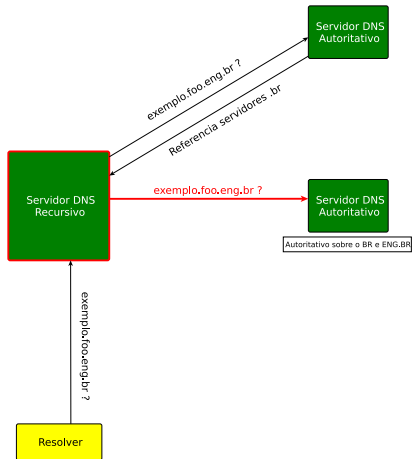


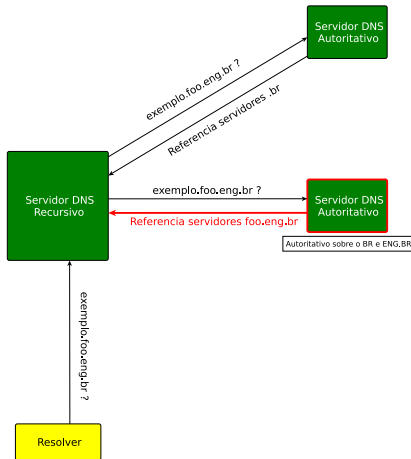
- O servidor DNS responde enviando DNSKEY e o RRSIG





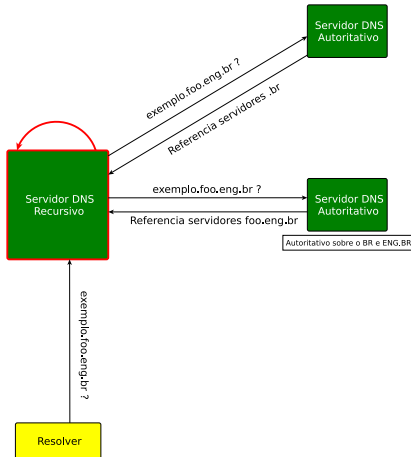
- Compara a trusted-key com a DNSKEY, caso for válida continua com as requisições

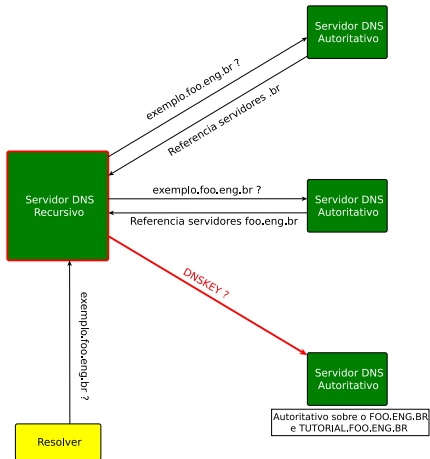


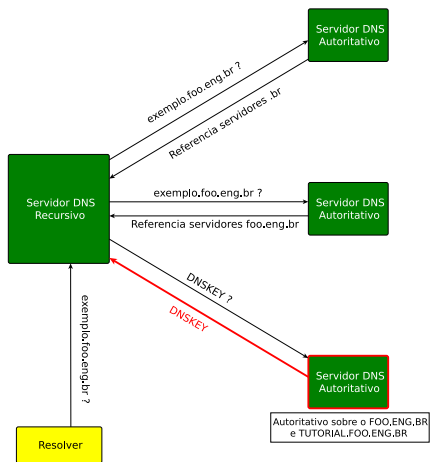


- Retorna sem resposta, mas com referência para os Records:
 - NS do “foo.eng.br”
- e com autoridade sobre os Records:
 - DS do “foo.eng.br”
 - RRSIG do Record DS

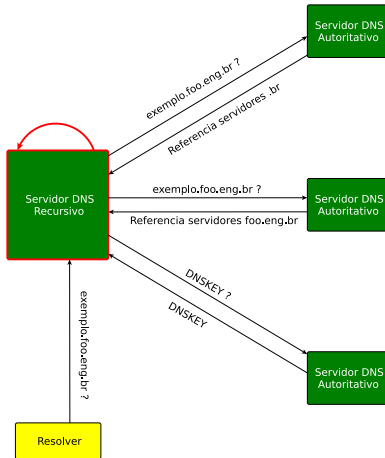
- O servidor DNS recursivo utiliza a DNSKEY para checar a assinatura (RRSIG) do Record DS

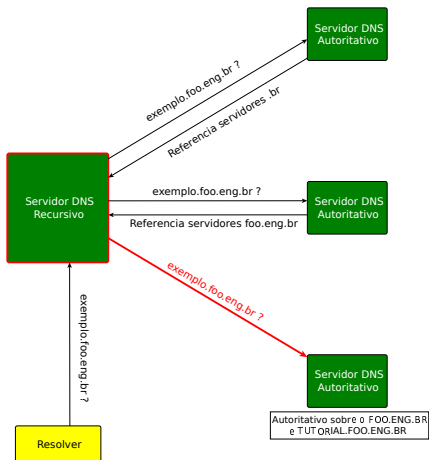




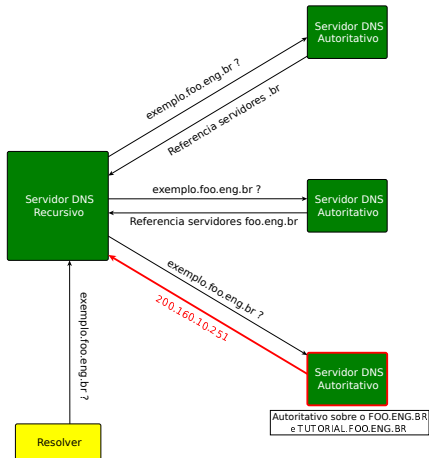


- O servidor DNS recursivo verifica através do DS e da DNSKEY, se este servidor DNS é válido.

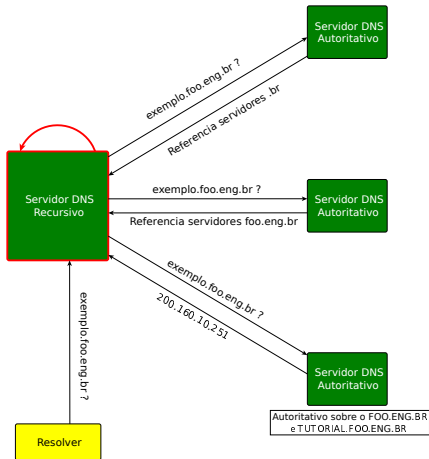


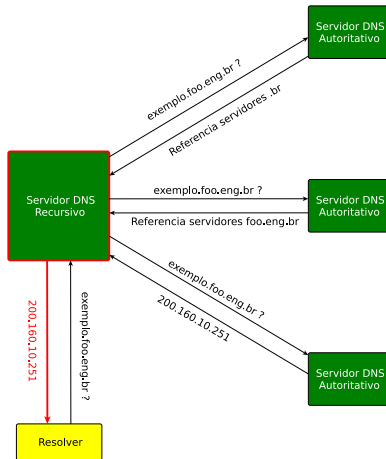


- Retorna o Record A e sua assinatura RRSIG.



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





Criado de forma a tornar mais flexíveis as limitações dos campos no protocolo DNS

- Permite aos solicitadores informarem a capacidade máxima de seus pacotes UDP. Eliminando a limitação UDP DNS de 512 bytes.
- Distingue quem suporta DNSSEC

Lembrete

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

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:

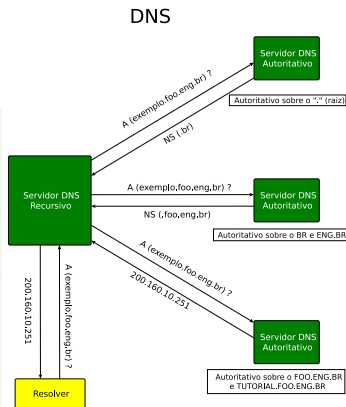
```
options {  
    edns-udp-size 1252; # Servidores recursivos  
    max-udp-size 1252; # Servidores recursivos e autoritativos  
};
```

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

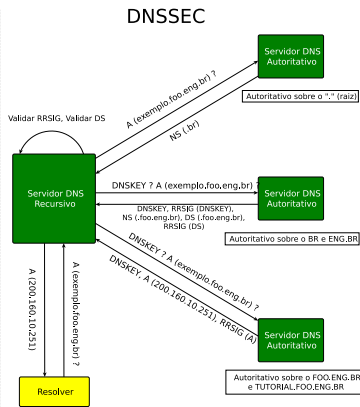
Recomendação

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

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



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

^a Versão atual do protocolo

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

^c Suporte a partir da versão 9.6.0

^d Suporte a partir da versão Windows Server 2008 R2 ou Windows 7

	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		✓	✓	✓	

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

^bApenas nas versões mais recentes do sistema operacional

^cSoftware 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 Idns 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”

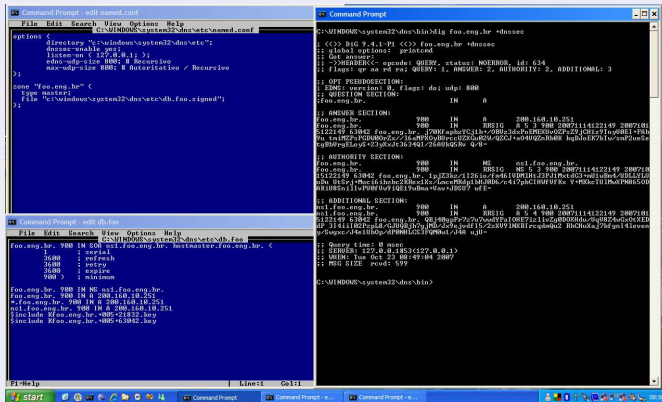
Erro ao iniciar o serviço ISC BIND

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

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`

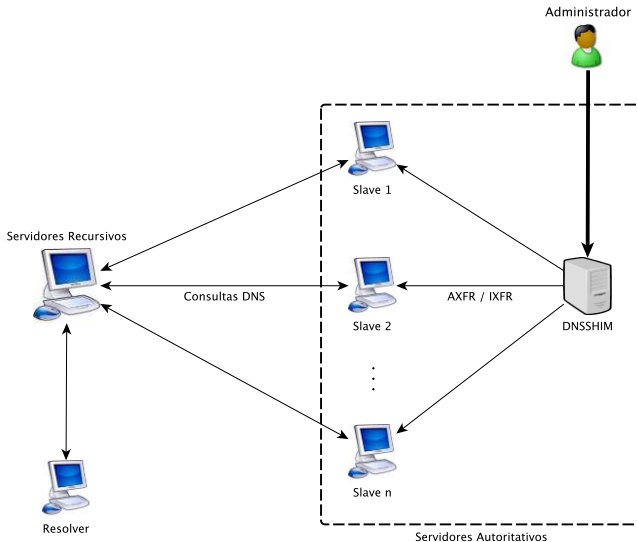


<http://registro.br/dnsshim/>

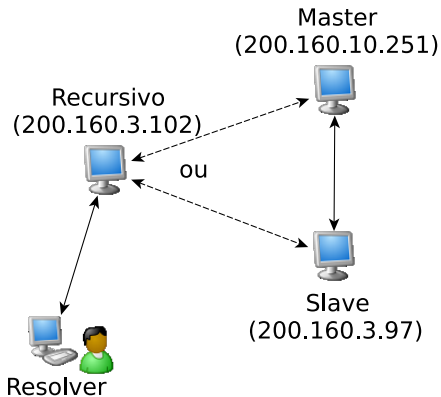
- Open-Source
- Automatiza o processo de provisionamento de zonas
- Suporte a DNSSEC
- Interface Automatizável
- Manutenção de chaves/assinaturas

Público Alvo

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



- 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
 - 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



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
```

```
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;
    };
};
```

```
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;  
    };  
};
```

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
```


Núcleo de Informação e Coordenação do Ponto br

[Home](#) [Registro](#) [Info](#) [FAQ](#) [Pesquisas](#) [Estatísticas](#) [Mapa](#) [Contato](#)

registro.br

Registro de Domínios
para a Internet no Brasil

[Alterar Cadastro do ID \[XXXX\]](#) | [Fechar Sessão](#)

Novos Domínios : [Institucional](#) | [Profissional Liberal](#) | [Pessoa Física](#)
[Sistema de IPs](#) | [Cancelar domínio](#) | [Tickets Processados](#)

Tela Principal

Id: XXXX

29/05/2008 09:20:45

☒ Novo ☒ Expirando ☐ Expirado ☒ Congelado

Administrativo	Técnico	Cobrança
Entidades		

cgi.br

Núcleo de Informação e Coordenação do Ponto br

[Home](#) [Registro](#) [Info](#) [FAQ](#) [Pesquisas](#) [Estatísticas](#) [Mapa](#) [Contato](#)

registro.br

Registro de Domínios
para a Internet no Brasil

[Tela Principal](#)

Novo Domínio PL

Id: XXXX
29/05/2008 09:58:48

Domínio

Domínio eng.br ▼

Período de registro 1 ano - R\$ 30,00 ▼

Informações do Profissional Liberal

CPF
(999.999.999-99)

Nome

Endereço

CEP
(99999-999)

Logradouro

Número Complemento

Cidade UF

Telefone

DDD Telefone Ramal

Informações sobre os Contatos

Administrativo XXXX

Técnico XXXX

Cobrança XXXX

Delegações DNS

Delegações DNS

É obrigatória a delegação dos servidores Master e Slave1.

Instruções para o preenchimento dos campos IP e IPv6. [Clique aqui.](#)

Servidor Master

Nome

Endereço IP

Endereço IPv6
(opcional)

Servidor Slave 1

Nome

Endereço IP

Endereço IPv6
(opcional)

Após estes procedimentos é necessário aguardar uma nova publicação

BIND: dnssec-keygen

Zona foo.eng.br:

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

Onde,

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

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

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

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

Exemplo de Tamanho de chaves

- BR: 1280 bits

Chave pública (.key)

```
foo.eng.br. IN DNSKEY 257 3 5 AwEAAaDaICi4nCQX+dC+kkGlGmi7+Pjww405WYZtt+oe1RG329H2+kOY XhYiZx7tLULD8Fn3DtBC
hGTeFND+gCBj0vFS9MEjxHIkD2gtt3fFibqN /sQIHDjNGr1M6aFngKxWTENWqk171hT9j0EvzsLOD+deFDge4sDF5qOQ 4D8njqIiIqDsU
kt3I1cJoFtP9k9RPIijxWdILWuKgh7nEvKpX7e0EuXO YK1W88Av9ctpm3y6lzsWCOK40I17nGTB+qMCbt/ZdYMwcaVuTBHQpEUKNVuq3m
FGJ1MxwtadBimmqq+YhleGzn21x0CYmsStwNUAWcb/H9SsqOG F3CVcH0t86k=
```

Chave privada (.private)

```
Private-key-format: v1.2
Algorithm: 5 (RSASHA1)
Modulus: 0NogKLicJBf50L6SQAuaLv4+PDDg7lZhm236h7VEbfb0fb6TRheFiJnHuOtQsPwWfc00EKEZN4U0P6AIGPS8VL0wSPEciQPac
23d8Uhuo3+xAgcOM0avUzpoWeArFZMQ1aqSXvWFP2M4S/Ows4P514U0B7iwMXmo5DgPye0Kogio0xSS3cjVwmgW0/2T1E8iKPFZ0gta4qCH
ucS8qlft44S5c5grVbzwC/1y2mbfLqXNuxYLQrg4iXucZMH6owJu39l1gzBxpW5MEdCkRQo1W6reYUaPUzHC1p0GKaaqr5iGV4b0fbXHQJi
axK3A1QBZxv8f1KqDQYXcJVwfs3zqQ==
```

...

OBS

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

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

BIND: dnssec-signzone

Zona foo.eng.br:

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

Onde,

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

Geração de records DS

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

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

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 chave da Zona “.” (Recursivo)

Obtendo a chave a ser ancorada (raiz)

<https://data.iana.org/root-anchors/>

- 1 Instalar o BIND, mantendo as configurações padrão
- 2 No arquivo named.conf, definir “dnssec-validation yes” (BIND 9.4 ou superior) nas opções
- 3 Obtenha a chave pública da zona . (raiz)
- 4 Inserir a chave pública no bloco denominado “managed-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
- A chave ancorada será automaticamente trocada ao ocorrer um “rollover” da chave da raiz, conforme a RFC 5011

Exemplo de inclusão de uma Chave

```
options {  
    directory "/etc/namedb";  
    pid-file "/var/run/named/pid";  
    dump-file "/var/dump/named_dump.db";  
    statistics-file "/var/stats/named.stats";  
    dnssec-validation yes; # BIND 9.4 ou superior  
    listen-on { 200.160.3.102; };  
};  
managed-keys {  
    . initial-key 257 3 8  
    "AwEAAgAIKlVZrpC6Ia7gEzah0R+9W29euxhJhVVL0yQ  
    bSEW008gcCjFFVQUTf6v58fLjwBd0YIOEzrAcQqBGCzh  
    /RStIo08gONfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWA  
    JQ9VnMVDxP/VHL496M/QZxkj5/Efucp2gaDX6RS6CXp  
    oY68LsvPVjROZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3  
    LQpzW5h0A2hzCTMjJPJ8LbqF6dsV6DoBQzguloSGicGO  
    Y170yQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8ONGC  
    LmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0=";  
};  
...
```

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/CCBfzH64yORAQf90xYDsI4xuBNaam+8DZQZ
                        xeoSLQEETwmp6wBtQ7G10wSM9nEjRRhbZdNPNKJMp2PE
                        lLLgLI+BLwdlz0t8MypcpL0aTm9rc7pP7UR5XLzU1k8D
                        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
                        U1UjOHUOHefajXzMv7F1FMWYeU51Ybg49HFe67XQV1K5
                        4GeAFXWB7YS59yODLoNEBxQ19QEY6g/00nLpuKTrST8q
                        qd5Fc/eYqN/Ag3GnfcAviZgiQhhveGH9mJHWZyc= )
```

Núcleo de Informação e Coordenação do Ponto br

[Home](#) [Registro](#) [Info](#) [FAQ](#) [Pesquisas](#) [Estatísticas](#) [Mapa](#) [Contato](#)**registro.br**Registro de Domínios
para a Internet no Brasil

Verificação de registros DS

Os campos abaixo devem ser preenchidos utilizando somente caracteres ASCII [a-zA-Z0-9-.]

Domínio

Servidor DNS (nome ou IP)

PESQUISAR**LIMPAR**

Records DS das chaves encontradas:

Key	Tag	Algoritmo	Digest	DS
-----	-----	-----------	--------	----

54964	RSA	/SHA1	F98A9B168BE481688E2E23771A9E6B79D425906E	(SHA1)
-------	-----	-------	--	--------

54964	RSA	/SHA1	6C1658EA2DF490472AA10020EFE9EDAAC6218BB7A31E9BD57A218479CBBE8B2E	(SHA256)
-------	-----	-------	--	----------

cgi.br

- Calcula o record DS a partir da DNSKEY

Apartir do arquivo dsset-foo.eng.br.

Records DS (preenchimento opcional)

Record DS 1

Key Tag Digest

----------------------	----------------------

Record DS 2

Key Tag D

foo.eng.br.

IN DS 34479 5 1

70E9E5267C3AE87F75742
AA6AF5EDCB442B93563

Após estes procedimentos é necessário aguardar uma nova publicação

- 1 Instalar BIND nos servidores
- 2 Configurar os arquivos de zona e named.conf no servidor Master e named.conf no servidores Slave
- 3 Executar o BIND (named) no servidores Master e Slave
- 4 Atualizar o registrar do domínio (com os records NS) e aguardar publicação
- 5 Realizar testes no servidor (DIG)
- 6 Criar chave (dnssec-keygen) (slide 109)
- 7 Assinar a zona (dnssec-signzone) (slide 111)
- 8 Atualizar o named.conf do servidor Master para utilizar o arquivo de zona .signed (slide 112)
- 9 Restartar o BIND (named) no servidores Master
- 10 Adicionar no “pai” o record DS (slide 117)
- 11 Aguardar nova publicação

- 1 Instalar BIND (com a biblioteca OpenSSL)
- 2 Obter a chave do site da IANA (slide 113)
- 3 Configurar o arquivo named.conf habilitando DNSSEC-VALIDATION (slide 114)
- 4 Incluir a managed-key no arquivo named.conf (slide 114)
- 5 Executar o BIND (named)

Recomendação

Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos

<http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/>

- 1 Instalar BIND com sigchase
- 2 Obter a chave do site da IANA (slide 113)
- 3 Incluir a chave no arquivo `/etc/trusted-key.key`
- 4 Realizar testes no servidor (`DIG +sigchase`)

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

A chave ancorada será automaticamente trocada conforme a RFC 5011

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.

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.

Por que existem dois tipos de chave?

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

Key Signing Key (KSK)

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

Zone Signing Key (ZSK)

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

Lembrete

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

Lembrete

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

Trabalhando com uma única chave!

Entretanto é aconselhável a utilização de somente uma única chave. Mais informações sobre como proceder no slide 111.

Inclusão dos Records DS das delegações

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

Exemplo

```
SHA1 tutorial.foo.eng.br. IN DS 3112 5 1 386B4390C5B30DB65D74EA8B660978077171948C
SHA256 tutorial.foo.eng.br. IN DS 3112 5 2
19602F6089F8877E037AA077B8376F30869E261EB55460F2A74E32AD1424F53A
```

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

foo.eng.br. IN NS ns1.foo.eng.br.
foo.eng.br. IN NS ns2.foo.eng.br.
...
tutorial.foo.eng.br. IN DS 3112 5 1 386B4390C5B30DB65D74EA8B660978077171948C
```

OBS

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



[RFC 2671](#)

Extension Mechanisms for DNS (EDNS0)



[RFC 2845](#)

Secret Key Transaction Authentication for DNS (TSIG)



[RFC 4033](#)

DNS Security Introduction and Requirements (DNSSEC-bis)



[RFC 4034](#)

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



[RFC 4035](#)

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



[RFC 4431](#)

The DNSSEC Lookaside Validation (DLV) DNS Resource Record



[RFC 4470](#)

Minimally Covering NSEC Records and DNSSEC On-line Signing



[RFC 4641](#)

DNSSEC Operational Practices



[RFC 5155](#)

DNSSEC Hashed Authenticated Denial of Existence

- ▶ **DNSSEC.NET**
<http://www.dnssec.net>
- ▶ **DNSSHIM**
<http://www.registro.br/dnsshim>
- ▶ **Wikipédia - DNSSEC**
<http://pt.wikipedia.org/wiki/DNSSEC>
- ▶ **Wikipédia - Comparação entre softwares de servidores DNS**
http://en.wikipedia.org/wiki/Comparison_of_DNS_server_software
- ▶ **Firewalls e DNS, como e porque configurar corretamente**
<ftp://ftp.registro.br/pub/doc/dns-fw.pdf>
- ▶ **Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos**
<http://www.cert.br/docs/whitepapers/dns-recursivo-aberto>
- ▶ **FAQ - Registro.br (Perguntas Frequentes)**
<http://registro.br/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!